Technical Report

FlexPod Implementation Guide

In Collaboration with Cisco

John George, Chris Reno, and Lindsey Street

For Internal and NetApp Partner Use Only

NetApp
January 2012 | TR-4019

TABLE OF CONTENTS

1 FLEXPOD OVERVIEW 5
1.1 AUDIENCE 5
1.2 FLEXPOD ARCHITECTURE 5
2 FLEXPOD CONFIGURATION VARIABLES 7
2.1 CONFIGURATION VARIABLES OVERVIEW 7
2.2 GLOBAL CONFIGURATION VARIABLES 8
2.3 NETAPP CONFIGURATION VARIABLES 9
2.4 CISCO CONFIGURATION VARIABLES 12
3 FLEXPOD DEPLOYMENT 14
3.1 CABLING INFORMATION 14
3.2 NETAPP FAS3240A DEPLOYMENT PROCEDURE: PART I 20
3.3 CISCO NEXUS 5548 DEPLOYMENT PROCEDURE: PART I 31
3.4 CISCO UNIFIED COMPUTING SYSTEM DEPLOYMENT PROCEDURE 42
3.5 GATHER NECESSARY INFORMATION 59
3.6 CISCO NEXUS 5548 DEPLOYMENT PROCEDURE: PART II 60
4 REFERENCES 65
5 REVISION HISTORY 65
6 AUTHORS 65

LIST OF TABLES

Table 1) FlexPod global variables. 8
Table 2) NetApp FAS3240A variables. 9
Table 3) NetApp licensing variables. 11
Table 4) NetApp disk and volume variables. 11
Table 5) Cisco Nexus 5548 variables. 12
Table 6) Cisco Unified Computing System variables. 12
Table 7) Cisco Nexus 5548 A Ethernet cabling information. 17
Table 8) Cisco Nexus 5548 B Ethernet cabling information. 17
Table 9) NetApp controller A Ethernet cabling information. 18
Table 10) NetApp controller B Ethernet cabling information. 18
Table 11) Cisco UCS fabric interconnect A Ethernet cabling information. 18
Table 12) Cisco UCS fabric interconnect B Ethernet cabling information. 19
Table 13) Cisco Nexus 5548 A Fibre Channel cabling information. 19
Table 14) Cisco Nexus 5548 B Fibre Channel cabling information. 19

Table 15) Cisco UCS fabric interconnect A Fibre Channel cabling information. 20
Table 16) Cisco UCS fabric interconnect B Fibre Channel cabling information. 20
Table 17) Assign controller disk ownership and initialize disk activity and verification. 20
Table 18) Set up Data ONTAP 8.0.1 activity and verification. 21
Table 19) Install Data ONTAP to the onboard flash storage activity and verification. 24
Table 20) Harden storage system logins and security activity and verification. 24
Table 21) Install required licenses activity and verification. 25
Table 22) Enable active-active controller configuration between the two storage systems activity and verification. 26
Table 23) Start FCP activity and verification. 26
Table 24) Set up storage system NTP time synchronization activity and verification. 26
Table 25) Add in-band management VLAN to 10GbE interfaces activity and verification. 27
Table 26) Create data aggregate `aggr1` activity and verification. 28
Table 27) Create SNMP requests role and assign SNMP login privileges activity and verification. 28
Table 28) Create SNMP management group and assign SNMP request role to its activity and verification. 28
Table 29) Create SNMP user and assign it to SNMP management group activity and verification. 29
Table 30) Enable SNMP on the storage controller's activity and verification. 29
Table 31) Set up an SNMP v1 community on the storage controller's activity and verification. 29
Table 32) Set SNMP contact information for each storage controller's activity and verification. 30
Table 33) Set SNMP location information for each storage controller's activity and verification. 30
Table 34) Reinitialize SNMP on storage controller's activity and verification. 30
Table 35) Enable Flash Cache activity and verification. 30
Table 36) Set up initial Cisco Nexus 5548 switch (controller A) activity and verification. 31
Table 37) Enable the appropriate Cisco Nexus licensing activity and verification. 32
Table 38) Set global configurations activity and verification. 33
Table 39) Create necessary VLANs activity and verification. 34
Table 40) Add individual port descriptions for troubleshooting activity and verification. 35
Table 41) Create necessary PortChannels activity and verification. 36
Table 42) Add PortChannel configurations activity and verification. 38
Table 43) Configure vPCs activity and verification. 40
Table 44) Uplink into existing network infrastructure activity and verification. 42
Table 45) Save configuration activity and verification. 42
Table 46) Initial setup of the Cisco UCS 6100 fabric interconnects activity and verification. 42
Table 47) Log in to Cisco UCS Manager activity and verification. 43
Table 48) Edit chassis discovery policy activity and verification. 43
Table 49) Enable Fibre Channel, server, and uplink ports activity and verification. 44
Table 50) Create an organization activity and verification. 45

Table 51) Create MAC address pools activity and verification. 45
Table 52) Create VLANs activity and verification. 46
Table 53) Create a network control policy activity and verification. 46
Table 54) Create a vNIC template activity and verification. 47
Table 55) Set jumbo frames in Cisco UCS Fabric activity and verification. 48
Table 56) Create uplink PortChannels to the Cisco Nexus 5548 switches activity and verification. 48
Table 57) Create WWNN pools activity and verification. 49
Table 58) Create WWPN pools activity and verification. 49
Table 59) Create VSANs and SAN PortChannels activity and verification. 50
Table 60) Create vHBA templates for fabric A and B activity and verification. 51
Table 61) Create boot policies activity and verification. 52
Table 62) Create server pools activity and verification. 54
Table 63) Create UUID suffix pools activity and verification. 55
Table 64) Create service profile templates activity and verification. 55
Table 65) Create service profiles activity and verification. 58
Table 66) Add a block of IP addresses for KVM access activity and verification. 59
Table 67) Synchronize Cisco UCS to NTP activity and verification. 59
Table 68) Add more blades to FlexPod unit activity and verification. 59
Table 69) NetApp FAS3240A FC portname information. 60
Table 70) Cisco UCS blade WWPN information. 60
Table 71) Create VSANs, assign FC ports to SAN PortChannels and appropriate VSANs, and turn on FC ports activity and verification. 61
Table 72) Create device aliases on each Cisco Nexus 5548 and create zones for each Cisco UCS host activity and verification. 63

LIST OF FIGURES

Figure 1) FlexPod components and connectivity for an FCoE-connected storage controller. 6
Figure 2) FlexPod components and connectivity for an FC and 10GbE-connected storage controller. 6
Figure 3) FlexPod cabling diagram. 16

1 FLEXPOD OVERVIEW

Industry trends indicate a vast data center transformation toward shared infrastructures. Enterprise customers are moving away from silos of information and toward shared infrastructures, to virtualized environments, and eventually to the cloud to increase agility and reduce costs.

FlexPod™ is a predesigned configuration that is built on the Cisco Unified Computing System™ (Cisco UCS™), Cisco Nexus® data center switches, NetApp® FAS storage components, and software from a range of partners. FlexPod can scale up for greater performance and capacity, or it can scale out for environments that need consistent, multiple deployments. FlexPod is a baseline configuration, but it also has the flexibility to be sized and optimized to accommodate many different use cases.

Cisco and NetApp have developed FlexPod as a platform that can address current virtualization needs and simplify their evolution to an IT-as-a-service (ITaaS) infrastructure. FlexPod serves as the infrastructure foundation on which hypervisors and bare metal use cases reside for a variety of IT solutions. For a detailed study of several practical solutions deployed on FlexPod, including virtual desktop infrastructure (VDI) with VMware® View™ and enhanced secure multi-tenancy, refer to NetApp Technical Report 3884, FlexPod Solutions Guide.

1.1 AUDIENCE

This document describes the basic architecture of the FlexPod infrastructure and also prescribes the procedure to prepare the infrastructure for either a hypervisor or a bare metal configuration. The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core FlexPod architecture.

1.2 FLEXPOD ARCHITECTURE

The FlexPod architecture is highly modular or podlike. Although each customer's FlexPod unit might vary in its exact configuration, once a FlexPod unit is built, it can easily be scaled as requirements and demand change. This includes both scaling up (adding additional resources within a FlexPod unit) and scaling out (adding additional FlexPod units).

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated building block for all virtualized and nonvirtualized solutions. FlexPod includes NetApp storage, Cisco Nexus networking, and the Cisco UCS in a single package in which the computing and storage fit in one data center rack, with the networking residing in a separate rack. For ease of deployment, this defined group of hardware is configured into the reference architecture described in this document.

Because of port density, the networking components can accommodate multiple FlexPod configurations and even span multiple data center racks, if necessary. Figure 1 shows the FlexPod components and the network connections for a Fibre Channel over Ethernet (FCoE)–based configuration. Figure 2 details a Fibre Channel (FC)–based configuration. Both designs are supported by NetApp and Cisco, but this document focuses on the FCoE configuration.

The default hardware prescribed in the FlexPod technical specification document includes:

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 6120 fabric interconnects
- Three chassis of Cisco UCS blades with two fabric extenders per chassis
- NetApp FAS3240A: Dual storage controllers in a single chassis

Figure 1) FlexPod components and connectivity for an FCoE-connected storage controller.

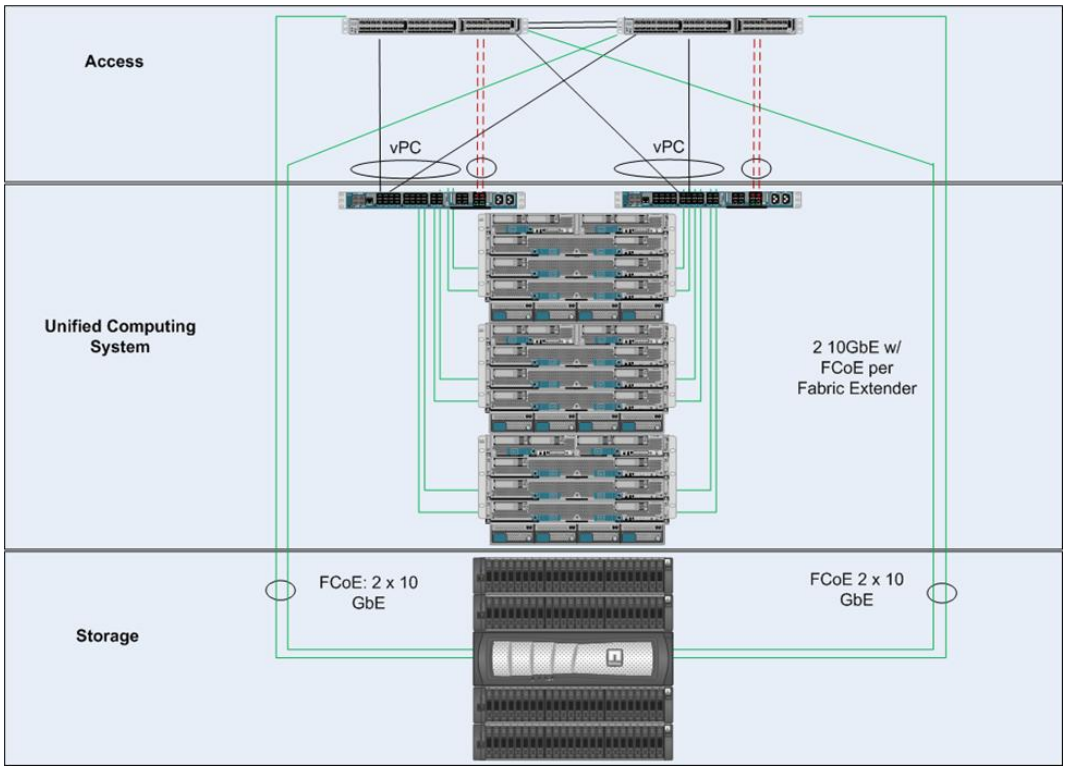
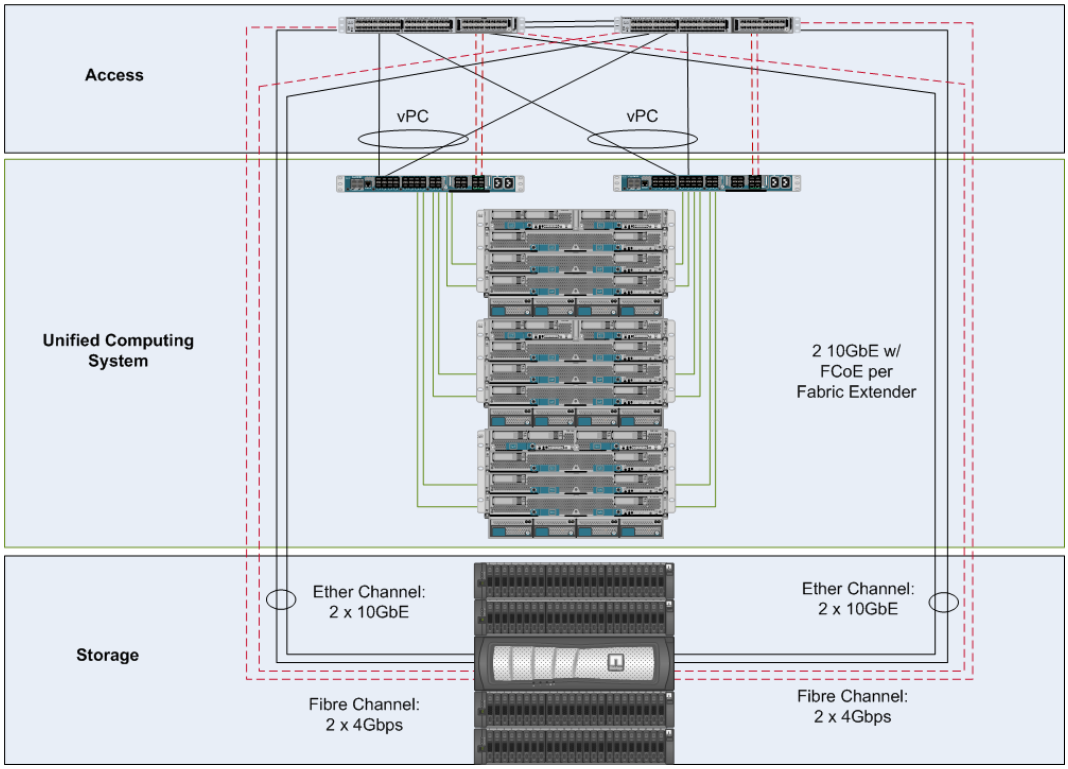


Figure 2) FlexPod components and connectivity for an FC and 10GbE-connected storage controller.



In the configurations shown in Figure 1 and Figure 2, storage is provided by a NetApp FAS3240A (high-availability [HA] configuration within a single chassis) with accompanying disk shelves. All systems and fabric links feature redundancy, providing for end-to-end HA. For virtualized and nonvirtualized workloads, the deployment could include hypervisor licenses or native operating system (OS) licenses, respectively. Although this is the default base design, each of the components can be scaled flexibly to support the specific business requirements of each case. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves could be deployed to improve storage I/O capacity and throughput, or special hardware or software features could be added to introduce new features (such as NetApp Flash Cache for dedupe-aware caching or VMware View for VDI deployments).

This document guides the reader through the low-level steps of deploying the base architecture, as shown in Figure 2. This includes everything from physical cabling to compute and storage configuration, to preparing the system for infrastructure volumes or datastores.

2 FLEXPOD CONFIGURATION VARIABLES

The following sections provide detailed deployment steps for building a standard FlexPod configuration. The deployment is split into several sections, depending on the equipment being configured: for example, NetApp FAS3240A storage controllers or Cisco Nexus 5548 switches. In each section, variables are introduced to allow professional services and partners to create a customized FlexPod implementation guide for their specific environment (using the Microsoft® Word [not the Adobe PDF] version of this document). After the variables have been customized, NetApp professional services and partners can use the implementation guide to configure a customized FlexPod environment that adheres to the best practices of Cisco and NetApp.

2.1 CONFIGURATION VARIABLES OVERVIEW

Variables are used throughout this document to help detail the deployment procedures to the customer's requirements and environment. Use the following procedure to create a customized document specific to each implementation.

1. Open the accompanying Microsoft Excel spreadsheet and fill in the Variable Values column with the appropriate customized values. Do not delete or edit any other content.
2. Save and close the updated spreadsheet.
3. Perform mail merge. This procedure varies depending on the version of Microsoft Word. Select the appropriate procedure from the following options:

For Microsoft Word 2007 (PC), complete the following steps:

a. Go to the Mailings tab in the top toolbar.
b. Click Select Recipients.
c. Click Use Existing List.
d. Navigate to and highlight the Excel spreadsheet saved in the previous steps. Click Open.
e. In the Select Table window, select MailMerge$, and click OK.
f. Click Finish & Merge on the right side of the top toolbar.
g. Select Edit Individual Documents.
h. Select All and click OK.
i. A new Word document is created and opened containing the customized variables provided. Be sure to save this document as necessary.

For Microsoft Word (Mac®):

a. Go to Tools, and then Mail Merge Manager.

b. Click Create New and select Form Letter.
c. Expand 2. Select Recipients List and click Get List.
d. Select Open Data Source.
e. Navigate to and highlight the Excel spreadsheet saved in the previous steps. Click Open.
f. A window displays stating, “This file needs to be opened by Excel Workbook text converter.” Click OK.
g. In the Open Workbook window that displays, select Mail Merge from the drop-down menu and click OK.
h. Expand 6. Complete Merge.
i. Click the second icon from the left, Merge to New Document.
j. A new Word document is created and opened containing the customized variables provided. Be sure to save this document as necessary.

2.2 GLOBAL CONFIGURATION VARIABLES

The variables shown in Table 1 are used throughout the deployment across multiple layers in the environment, so they are considered global variables.

Table 1) FlexPod global variables.

Variable Name	Customized Value	Description
VLAN ID for management traffic	«var_global_mgmt_vlan_id»	Provide appropriate VLAN ID to be used for management traffic throughout FlexPod environment.
VLAN ID for native VLAN	«var_global_native_vlan_id»	Provide appropriate VLAN ID to be used for native VLAN ID throughout FlexPod environment.
Default password	«var_global_default_passwd»	Provide default password to be used in initial configuration of environment. **Note:** NetApp recommends changing this password as needed on each device after initial configuration is complete.
DNS server name	«var_global_nameserver_ip»	Provide IP address of appropriate name server for environment.
Domain name suffix	«var_global_domain_name»	Provide appropriate domain name suffix for environment.
VSAN ID for fabric A	«var_global_vsan_A_id»	Provide VSAN ID to be associated with fabric A. This is associated with both FC and FCoE traffic for fabric A.
VSAN ID for fabric B	«var_global_vsan_B_id»	Provide VSAN ID to be associated with fabric B. This is associated with both FC and FCoE traffic for fabric B.
FCoE VLAN ID for fabric A	«var_global_fcoe_A_vlan_id»	Provide VLAN ID of the VLAN to be mapped to FCoE traffic on fabric A.
FCoE VLAN ID for fabric B	«var_global_fcoe_B_vlan_id»	Provide VLAN ID of the VLAN to be mapped to FCoE traffic on fabric B.

Variable Name	Customized Value	Description
SSL country name code	«var_global_ssl_country»	Provide appropriate SSL country name code.
SSL state or province name	«var_global_ssl_state»	Provide appropriate SSL state or province name.
SSL locality name	«var_global_ssl_locality»	Provide appropriate SSL locality name (city, town, and so on).
SSL organization name	«var_global_ssl_org»	Provide appropriate SSL organization name (company name).
SSL organization unit	«var_global_ssl_org_unit»	Provide appropriate SSL organization unit (division).
NTP server IP address	«var_global_ntp_server_ip»	Provide NTP server IP address.

2.3 NETAPP CONFIGURATION VARIABLES

Table 2, Table 3, and Table 4 show the variables that are specific to the NetApp portion of the deployment only.

Table 2) NetApp FAS3240A variables.

Variable Name	Customized Value	Description
FAS3240A host name	«var_ntap_A_hostname»	Provide host name for NetApp FAS3240A.
FAS3240B host name	«var_ntap_B_hostname»	Provide host name for NetApp FAS3240B.
FAS3240A out-of-band (OOB) management IP	«var_ntap_A_mgmt_int_IP»	Provide IP address for out-of-band management interface on NetApp FAS3240A.
FAS3240B OOB management IP	«var_ntap_B_mgmt_int_IP»	Provide IP address for out-of-band management interface on NetApp FAS3240B.
FAS3240A OOB management subnet mask	«var_ntap_A_mgmt_int_netmask»	Provide subnet mask for out-of-band management interface on NetApp FAS3240A.
FAS3240B OOB management subnet mask	«var_ntap_B_mgmt_int_netmask»	Provide subnet mask for out-of-band management interface on NetApp FAS3240B.
FAS3240A management gateway	«var_ntap_A_mgmt_int_gw»	Provide gateway IP address for management interface on NetApp FAS3240A.
FAS3240B management gateway	«var_ntap_B_mgmt_int_gw»	Provide gateway IP address for management interface on NetApp FAS3240B.
FAS3240A in-band management IP	«var_ntap_A_ib_mgmt_IP»	Provide IP address for in-band (10GbE) management interface on NetApp FAS3240A.
FAS3240B in-band management IP	«var_ntap_B_ib_mgmt_IP»	Provide IP address for in-band (10GE) management interface on NetApp FAS3240B.

Variable Name	Customized Value	Description
FAS3240A in-band management subnet mask	«var_ntap_A_ib_mgmt_netmask»	Provide subnet mask for in-band (10GE) management interface on NetApp FAS3240A.
FAS3240B in-band management subnet mask	«var_ntap_B_ib_mgmt_netmask»	Provide subnet mask for in-band (10GE) management interface on NetApp FAS3240B.
FAS3240 administration host	«var_ntap_admin_host_ip»	Provide IP address of host to be used for administering NetApp FAS3240s.
FAS3240 location	«var_ntap_location»	Provide a description of physical location where NetApp chassis resides.
NetApp FAS3240A service processor interface IP address	«var_ntap_A_sp_int_ip»	Provide IP address for service processor interface on NetApp FAS3240A.
NetApp FAS3240B service processor interface IP address	«var_ntap_B_sp_int_ip»	Provide IP address for service processor interface on NetApp FAS3240B.
NetApp FAS3240A service processor interface subnet mask	«var_ntap_A_sp_int_netmask»	Provide subnet mask for service processor interface on NetApp FAS3240A.
NetApp FAS3240B service processor interface subnet mask	«var_ntap_B_sp_int_netmask»	Provide subnet mask for service processor interface on NetApp FAS3240B.
NetApp FAS3240A service processor interface gateway IP address	«var_ntap_A_sp_int_gw»	Provide gateway IP address for service processor interface on NetApp FAS3240A.
NetApp FAS3240B service processor interface gateway IP address	«var_ntap_B_sp_int_gw»	Provide gateway IP address for service processor interface on NetApp FAS3240B.
NetApp FAS3240A mailhost name	«var_ntap_mailhost_name»	Provide appropriate mail host name.
NetApp FAS3240A mail host IP address	«var_ntap_mailhost_ip»	Provide appropriate mail host IP address.
NetApp Data ONTAP® 8.0.1 flash image location	«var_ntap_data_ontap_url»	Provide http or https Web address of NetApp Data ONTAP 8.0.1 flash image to install image to onboard flash storage.
NetApp FAS3240A administrator's e-mail address	«var_ntap_admin_email_address»	Provide e-mail address for NetApp administrator to receive important alerts/messages by e-mail.
SNMP v1 read-only community string	«var_ntap_snmp_community»	Provide SNMP v1 read-only community string for storage controllers so that OnCommand™ System Manager can be used to manage storage systems.

Variable Name	Customized Value	Description
SNMP username	«var_ntap_snmp_user»	Provide appropriate SNMP username.
SNMP password	«var_ntap_snmp_password»	Provide appropriate SNMP password.
SNMP request role	«var_ntap_snmp_request_role»	Provide request role for SNMP.
SNMP managers	«var_ntap_snmp_managers»	Provide users who have ability to manage SNMP.
SNMP site name	«var_ntap_snmp_site_name»	Provide site name as required by SNMP.

Table 3) NetApp licensing variables.

Variable Name	Customized Value	Description
NetApp cluster license code	«var_ntap_cluster_lic»	Provide license code to enable Cluster-Mode within FAS3240A configuration.
NetApp Fibre Channel license code	«var_ntap_fcp_lic»	Provide license code to enable FC protocol.
NetApp Flash Cache license code	«var_ntap_flash_cache_lic»	Provide license code to enable installed Flash Cache adapter.

Table 4) NetApp disk and volume variables.

Variable Name	Customized Value	Description
NetApp FAS3240A total disks attached	«var_ntap_A_num_disks»	Number of disks assigned to controller A using software ownership. **Note:** Do not include three disks used for root volume in this number.
NetApp FAS3240B total disks attached	«var_ntap_B_num_disks»	Number of disks assigned to controller B using software ownership. **Note:** Do not include three disks used for root volume in this number.
NetApp FAS3240A total disks in aggregate 1	«var_ntap_A_num_disks_aggr1»	Number of disks to be assigned to `aggr1` on controller A.
NetApp FAS3240B total disks in aggregate 1	«var_ntap_B_num_disks_aggr1»	Number of disks to be assigned to `aggr1` on controller B.

2.4 CISCO CONFIGURATION VARIABLES

Table 5 and Table 6 show the variables that are specific only to the Cisco® portion of the deployment.

Table 5) Cisco Nexus 5548 variables.

Variable Name	Customized Value	Description
Cisco Nexus 5548 A host name	«var_nexus_A_hostname»	Provide host name for Cisco Nexus 5548 A.
Cisco Nexus 5548 B host name	«var_nexus_B_hostname»	Provide host name for Cisco Nexus 5548 B.
Cisco Nexus 5548 A management interface IP address	«var_nexus_A_mgmt0_IP»	Provide IP address for mgmt0 interface on Cisco Nexus 5548 A.
Cisco Nexus 5548 B management interface IP address	«var_nexus_B_mgmt0_IP»	Provide IP address for mgmt0 interface on Cisco Nexus 5548 B.
Cisco Nexus 5548 A management interface subnet mask	«var_nexus_A_mgmt0_netmask»	Provide subnet mask for mgmt0 interface on Cisco Nexus 5548 A.
Cisco Nexus 5548 B management interface subnet mask	«var_nexus_B_mgmt0_netmask»	Provide subnet mask for mgmt0 interface on Cisco Nexus 5548 B.
Cisco Nexus 5548 A management interface gateway IP address	«var_nexus_A_mgmt0_gw»	Provide gateway IP address for mgmt0 interface on Cisco Nexus 5548 A.
Cisco Nexus 5548 B management interface gateway IP address	«var_nexus_B_mgmt0_gw»	Provide the gateway IP address for the mgmt0 interface on Cisco Nexus 5548 B.
Cisco Nexus 5548 virtual PortChannel (vPC) domain ID	«var_nexus_vpc_domain_id»	Provide unique vPC domain ID for environment.

Table 6) Cisco Unified Computing System variables.

Variable Name	Customized Value	Description
Cisco UCS fabric interconnect A host name	«var_ucsm_A_hostname»	Provide host name for fabric interconnect A.
Cisco UCS fabric interconnect B host name	«var_ucsm_B_hostname»	Provide host name for fabric interconnect B.
Cisco UCS name	«var_ucsm_cluster_hostname»	Both Cisco UCS fabric interconnects are clustered together as a single Cisco UCS. Provide host name for clustered system.

Variable Name	Customized Value	Description
Cisco UCS IP	«var_ucsm_cluster_ip»	Both Cisco UCS fabric interconnects are clustered together as a single Cisco UCS. Provide IP address for clustered system.
Cisco UCS fabric interconnect A management interface IP address	«var_ucsm_A_mgmt_ip»	Provide IP address for fabric interconnect A's management interface.
Cisco UCS fabric interconnect B management interface IP address	«var_ucsm_B_mgmt_ip»	Provide IP address for fabric interconnect B's management interface.
Cisco UCS fabric interconnect A management netmask	«var_ucsm_A_mgmt_netmask»	Provide subnet mask for fabric interconnect A's management interface.
Cisco UCS fabric interconnect B management interface netmask	«var_ucsm_B_mgmt_netmask»	Provide subnet mask for fabric interconnect B's management interface.
Cisco UCS fabric interconnect A management interface gateway	«var_ucsm_A_mgmt_gw»	Provide gateway IP address for fabric interconnect A's management interface.
Cisco UCS fabric interconnect B management interface gateway	«var_ucsm_B_mgmt_gw»	Provide gateway IP address for fabric interconnect B's management interface.
Cisco UCS infrastructure organization	«var_ucsm_infra_org_name»	A Cisco UCS organization is created for necessary "infrastructure" resources. Provide a descriptive name for this organization.
Starting mandatory access control (MAC) address for fabric A	«var_ucsm_mac_pool_A_start»	A pool of MAC addresses is created for each fabric. Depending on environment, certain MAC addresses might already be allocated. Identify a unique MAC address as starting address in MAC pool for fabric A. If possible, NetApp recommends using either 0A or 0B as second-to-last octet to help distinguish MACs on fabric A from those on fabric B.
Starting MAC address for fabric B	«var_ucsm_mac_pool_B_start»	A pool of MAC addresses is created for each fabric. Depending on environment, certain MAC addresses might already be allocated. Identify a unique MAC address as starting address in MAC pool for fabric B. If possible, NetApp recommends using either 0A or 0B as second-to-last octet to help distinguish MACs on fabric A from those on fabric B.

Variable Name	Customized Value	Description
Starting WWPN for fabric A	«var_ucsm_wwpn_pool_A_start»	A pool of worldwide portnames (WWPNs) is created for each fabric. Depending on environment, certain WWPNs might already be allocated. Identify a unique WWPN as starting point in WWPN pool for fabric A. If possible, NetApp recommends using either 0A or 0B as second-to last-octet to help distinguish WWPNs on fabric A from those on fabric B.
Starting WWPN for fabric B	«var_ucsm_wwpn_pool_B_start»	A pool of WWPNs is created for each fabric. Depending on environment, certain WWPNs might already be allocated. Identify a unique WWPN as starting point in WWPN pool for fabric B. If possible, NetApp recommends using either 0A or 0B as second-to-last octet to help distinguish WWPNs on fabric A from those on fabric B.

3 FLEXPOD DEPLOYMENT

The following section provides detailed information about configuring all aspects of a base FlexPod environment. At the end of these deployment steps, the end user is prepared to install an OS on two Cisco UCS hosts. The outlined procedure includes:

- Initial NetApp controller configuration
- Initial Cisco UCS configuration
- Initial Cisco Nexus configuration
- Creation of necessary VLANs and VSANs for management and basic functionality
- Creation of necessary vPCs to provide HA among devices
- Creation of necessary service profile pools: WWPN, worldwide node name (WWNN), MAC, server, and so forth
- Creation of necessary service profile policies: adapter, boot, and so forth
- Creation of two service profile templates from the created pools and policies: one each for fabric A and B
- Provisioning of two servers from the created service profiles in preparation for OS installation

The FlexPod architecture is flexible; therefore, the exact configuration detailed in this section might vary for customer implementations, depending on specific requirements. Although customer implementations might deviate from the information that follows, the best practices, features, and configurations listed in this section should still be used as a reference for building a customized FlexPod architecture.

3.1 CABLING INFORMATION

The following information is provided as a reference for cabling the physical equipment in a FlexPod environment. The tables include both local and remote device and port locations in order to simplify cabling requirements.

The tables in this section contain details for the prescribed and supported configuration of the FAS3240 running Data ONTAP 8.0.1. This configuration leverages a dual-port 10GbE add-on Unified Target

Adapter (UTA) and the onboard SAS ports for disk shelf connectivity. For any modifications of this prescribed architecture, consult the currently available Interoperability Matrix Tool (IMT).

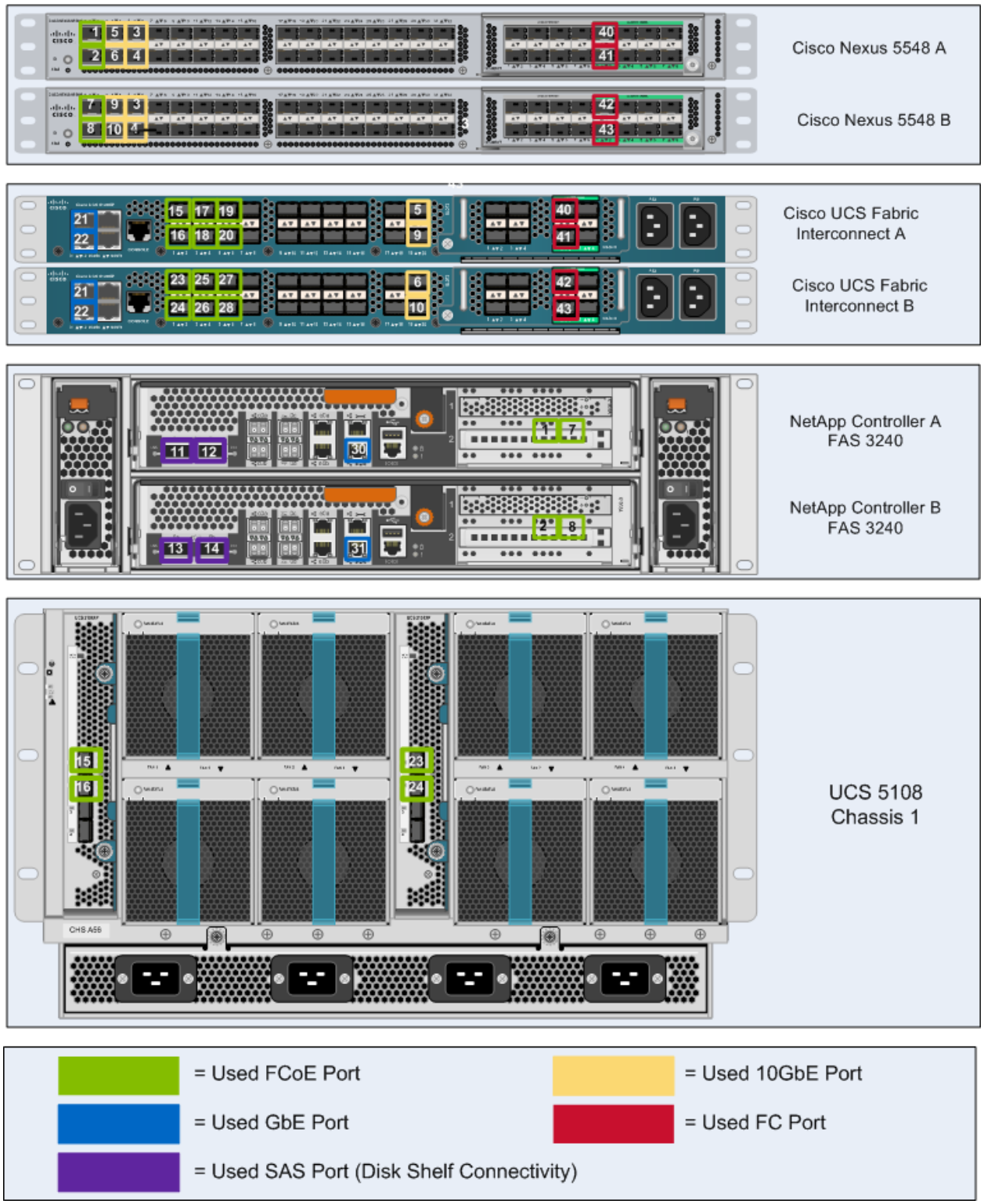
Note: This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

Note: Be sure to follow the cable directions in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned.

Note: It is possible to order a FAS3240A system in a different configuration from what is prescribed in the tables in this section. Before starting, be sure the configuration matches what is described in the tables and diagrams in this section

Figure 3 shows a FlexPod cabling diagram. The labels indicate connections to endpoints rather than port numbers on the physical device. For example, connection 1 is an FCoE target port connected from NetApp controller A to Cisco Nexus 5548 A. SAS connections 11, 12, 13, and 14 as well as ACP connections 30 and 31 should be connected to the NetApp storage controller and disk shelves according to best practices for the specific storage controller and disk shelf quantity.

Figure 3) FlexPod cabling diagram.


Cisco Nexus 5548 A
Cisco Nexus 5548 B
Cisco UCS Fabric Interconnect A
Cisco UCS Fabric Interconnect B
NetApp Controller A FAS 3240
NetApp Controller B FAS 3240
UCS 5108 Chassis 1
= Used FCoE Port
= Used 10GbE Port
= Used GbE Port
= Used FC Port
= Used SAS Port (Disk Shelf Connectivity)

The physical ports and their corresponding endpoints for Ethernet, FCoE, and FC-based traffic are listed in Table 7 through Table 12.

Table 7) Cisco Nexus 5548 A Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A – «var_nexus_A_hostname»	Eth1/1	FCoE/10GbE	NetApp controller A – «var_ntap_A_hostname»	e2a
	Eth1/2	FCoE/10GbE	NetApp controller B – «var_ntap_B_hostname»	e2a
	Eth1/5	10GbE	Cisco Nexus 5548 B – «var_nexus_B_hostname»	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 B – «var_nexus_B_hostname»	Eth1/6
	Eth1/3	10GbE	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Eth1/19
	Eth1/4	10GbE	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Eth1/19
	MGMT0	100MbE	100MbE management switch	Any

Note: For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC–T=).

Table 8) Cisco Nexus 5548 B Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B – «var_nexus_B_hostname»	Eth1/1	FCoE/10GbE	NetApp controller A «var_ntap_A_hostname»	e2b
	Eth1/2	FCoE/10GbE	NetApp controller B «var_ntap_B_hostname»	e2b
	Eth1/5	10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/6
	Eth1/3	10GbE	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Eth1/20
	Eth1/4	10GbE	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Eth1/20
	MGMT0	100MbE	100MbE management switch	Any

Note: For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC–T=).

Table 9) NetApp controller A Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller A – «var_ntap_A_hostname»	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e2a	FCoE/10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/1
	e2b	FCoE/10GbE	Cisco Nexus 5548 B «var_nexus_B_hostname»	Eth1/1

Table 10) NetApp controller B Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller B – «var_ntap_B_hostname»	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e2a	FCoE/10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/2
	e2b	FCoE/10GbE	Cisco Nexus 5548 B «var_nexus_B_hostname»	Eth1/2

Table 11) Cisco UCS fabric interconnect A Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Eth1/19	10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/3
	Eth1/20	10GbE	Cisco Nexus 5548 B «var_nexus_B_hostname»	Eth1/3
	Eth1/1	FCoE/10GbE	Chassis 1 FEX A	Port 1
	Eth1/2	FCoE/10GbE	Chassis 1 FEX A	Port 2
	Eth1/3	FCoE/10GbE	Chassis 2 FEX A	Port 1
	Eth1/4	FCoE/10GbE	Chassis 2 FEX A	Port 2
	Eth1/5	FCoE/10GbE	Chassis 3 FEX A	Port 1
	Eth1/6	FCoE/10GbE	Chassis 3 FEX A	Port 2
	MGMT0	100MbE	100MbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	L1
	L2	GbE	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	L2

Table 12) Cisco UCS fabric interconnect B Ethernet cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Eth1/19	10GbE	Cisco Nexus 5548 A «var_nexus_A_hostname»	Eth1/4
	Eth1/20	10GbE	Cisco Nexus 5548 B «var_nexus_B_hostname»	Eth1/4
	Eth1/1	10GbE/FCoE	Chassis 1 FEX B	Port 1
	Eth1/2	10GbE/FCoE	Chassis 1 FEX B	Port 2
	Eth1/3	10GbE/FCoE	Chassis 2 FEX B	Port 1
	Eth1/4	10GbE/FCoE	Chassis 2 FEX B	Port 2
	Eth1/5	10GbE/FCoE	Chassis 3 FEX B	Port 1
	Eth1/6	10GbE/FCoE	Chassis 3 FEX B	Port 2
	MGMT0	100MbE	100MbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	L1
	L2	GbE	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	L2

The FlexPod FC cabling information is contained in Table 13 through Table 16.

Table 13) Cisco Nexus 5548 A Fibre Channel cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A – «var_nexus_A_hostname»	Fc2/1	FC	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Fc2/1
	Fc2/2	FC	Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Fc2/2

Table 14) Cisco Nexus 5548 B Fibre Channel cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B – «var_nexus_B_hostname»	Fc2/1	FC	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Fc2/1
	Fc2/2	FC	Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Fc2/2

Table 15) Cisco UCS fabric interconnect A Fibre Channel cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A – «var_ucsm_A_hostname»	Fc2/1	FC	Cisco Nexus 5548 A «var_nexus_A_hostname»	Fc2/1
	Fc2/2	FC	Cisco Nexus 5548 A «var_nexus_A_hostname»	Fc2/2

Table 16) Cisco UCS fabric interconnect B Fibre Channel cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B – «var_ucsm_B_hostname»	Fc2/1	FC	Cisco Nexus 5548 B «var_nexus_B_hostname»	Fc2/1
	Fc2/2	FC	Cisco Nexus 5548 B «var_nexus_B_hostname»	Fc2/2

3.2 NETAPP FAS3240A DEPLOYMENT PROCEDURE: PART I

The following section provides a detailed procedure for configuring the NetApp FAS3240A for use in a FlexPod environment. These steps should be followed precisely. Failure to do so could result in an improper configuration.

ASSIGN CONTROLLER DISK OWNERSHIP AND INITIALIZE DISKS

Table 17) Assign controller disk ownership and initialize disk activity and verification.

Activity	Verification
Assign controller disk ownership and initialize disks.	Type `disk show` on the command line for each controller to generate a list of disks owned by each respective controller.

Controller A – «var_ntap_A_hostname»

1. During controller boot, when prompted to press CTRL-C for Boot Menu, press CTRL-C.
2. At the menu prompt, select option 5 for Maintenance mode boot.
3. Type `Yes` if prompted with `Continue to boot?`
4. Type `disk show`. No disks should be assigned to the controller.
5. Reference the `Local System ID:` value for the following disk assignment.

Note: Half of the total number of disks in the environment are assigned to this controller and half to the other controller. Divide the number of disks in half and use the result in the following command for the <# of disks>.

6. Type `disk assign -n «var_ntap_A_num_disks»`.
7. Type `halt` to reboot the controller.
8. If the controller stops at a LOADER–A> prompt, type `autoboot` to start Data ONTAP.
9. During controller boot, when prompted to `Press CTRL-C for Boot Menu`, press CTRL-C.
10. At the menu prompt, select option 4 for Clean configuration and initialize all disks.

11. The installer asks if you want to zero the disks and install a new file system. Answer `y`.
12. A warning displays that this will erase all of the data on the disks. Answer `y` that you are sure this is what you want to do.

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. Once initialization is complete, the storage system reboots.

Controller B – «var_ntap_B_hostname»

1. During controller boot, when prompted to press CTRL-C for special boot menu, press CTRL-C.
2. At the menu prompt, select option 5 for Maintenance mode boot.
3. Type `Yes` if prompted with `Continue to boot?`
4. Type `disk show`. No disks should be assigned to the controller.
5. Reference the `Local System ID:` value for the following disk assignment.

Note: Half of the total number of disks in the environment are assigned to this controller and half to the other controller. Divide the number of disks in half and use the result in the following command for the <# of disks>.

6. Type `disk assign –n «var_ntap_B_num_disks»`.
7. Type `halt` to reboot the controller.
8. If the controller stops at a `LOADER-B>` prompt, type `autoboot` to start Data ONTAP.
9. During controller boot, when prompted to press CTRL-C for Boot Menu, press CTRL-C.
10. At the menu prompt, select option 4 for Clean configuration and initialize all disks.
11. The installer asks if you want to zero the disks and install a new file system. Answer `y`.
12. A warning displays that this will erase all of the data on the disks.
13. Answer `y` that you are sure this is what you want to do.

Note: The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. Once initialization is complete, the storage system reboots.

SET UP DATA ONTAP 8.0.1

Table 18) Set up Data ONTAP 8.0.1 activity and verification.

Activity	Verification
Set up Data ONTAP 8.0.1. Duration: 15 minutes	To verify the successful setup of Data ONTAP 8.0.1, make sure that the terminal prompt is available and check the settings that were entered in the setup wizard.

Controller A – «var_ntap_A_hostname»

1. After the disk initialization and the creation of the root volume, Data ONTAP setup begins.
2. Enter `«var_ntap_A_hostname»` for the host name of the storage system.
3. Answer `y` for setting up interface groups.
4. Enter `1` for the number of interface groups to configure.
5. Name the interface `vif0`.
6. Enter `l` to specify the interface as LACP.
7. Enter `2` for the number of links for `vif0`.

8. Enter `e2a` for the name of the first link.
9. Enter `e2b` for the name of the second link.
10. Press `Enter` when prompted for an IP address for `vif0` to accept the blank IP address.
11. Enter `n` for interface group `vif0` taking over a partner interface.
12. Enter «`var_ntap_A_mgmt_int_IP`» for the IP address of the management interface, `e0M`.
13. Enter «`var_ntap_A_mgmt_int_netmask`» as the subnet mask for `e0M`.
14. Enter `y` for interface `e0M` taking over a partner IP address during failover.
15. Enter `e0M` for the name of the interface to be taken over.
16. Press Enter to accept the default flow control of `full`.
17. Press Enter to accept the blank IP address for `e0a`.
18. Enter `n` for interface `e0a` taking over a partner interface.
19. Press Enter to accept the blank IP address for `e0b`.
20. Enter `n` for interface `e0b` taking over a partner interface.
21. Answer `n` to continuing setup through the Web interface.
22. Enter «`var_ntap_A_mgmt_int_gw`» as the IP address for the default gateway for the storage system.
23. Enter «`var_ntap_admin_host_ip`» as the IP address for the administration host.
24. Enter the local timezone (for example, PST, MST, CST, or EST).
25. Enter «`var_ntap_location`» as the location for the storage system.
26. Answer `y` to enable DNS resolution.
27. Enter «`var_global_domain_name`» as the DNS domain name.
28. Enter «`var_global_nameserver_ip`» as the IP address for the first nameserver.
29. Answer `n` to finish entering DNS servers, or answer `y` to add up to two more DNS servers.
30. Answer `n` for running the NIS client.
31. Press Enter to acknowledge the AutoSupport™ message.
32. Answer `y` to configuring the SP LAN interface.
33. Answer `n` to setting up DHCP on the SP LAN interface.
34. Enter «`var_ntap_A_sp_int_ip`» as the IP address for the SP LAN interface.
35. Enter «`var_ntap_A_sp_int_netmask`» as the subnet mask for the SP LAN interface.
36. Enter «`var_ntap_A_sp_int_gw`» as the IP address for the default gateway for the SP LAN interface.
37. Enter «`var_ntap_mailhost_name`» as the name for the mail host to receive SP messages and AutoSupport.
38. Enter «`var_ntap_mailhost_ip`» as the IP address for the mail host to receive SP messages and AutoSupport.
39. Enter «`var_global_default_passwd`» for the new administrative (root) password.
40. Enter «`var_global_default_passwd`» again to confirm the new administrative (root) password.
41. After these steps are completed, the controller should display a password prompt. Enter «`var_global_default_passwd`» to log in as root.

Controller B – «var_ntap_B_hostname»

1. After the disk initialization and the creation of the root volume, the Data ONTAP setup begins.

2. Enter «var_ntap_B_hostname» for the host name of the storage system.
3. Answer y for setting up interface groups.
4. Enter 1 for the number of interface groups to configure.
5. Name the interface vif0.
6. Enter l to specify the interface as LACP.
7. Enter 2 for the number of links for vif0.
8. Enter e2a for the name of the first link.
9. Enter e2b for the name of the second link.
10. Press Enter when prompted for an IP address for vif0 to accept the blank IP address.
11. Enter n for interface group vif0 taking over a partner interface.
12. Enter «var_ntap_B_mgmt_int_IP» for the IP address of the management interface, e0M.
13. Enter «var_ntap_B_mgmt_int_netmask» as the subnet mask for e0M.
14. Enter y for interface e0M taking over a partner IP address during failover.
15. Enter e0M for the name of the interface to be taken over.
16. Press Enter to accept the default flow control of full.
17. Press Enter to accept the blank IP address for e0a.
18. Enter n for interface e0a taking over a partner interface.
19. Press Enter to accept the blank IP address for e0b.
20. Enter n for interface e0b taking over a partner interface.
21. Answer n to continue setup through the Web interface.
22. Enter «var_ntap_B_mgmt_int_gw» as the IP address for the default gateway for the storage system.
23. Enter «var_ntap_admin_host_ip» as the IP address for the administration host.
24. Enter the local timezone (for example, PST, MST, CST, EST).
25. Enter «var_ntap_location» as the location for the storage system.
26. Answer y to enable DNS resolution.
27. Enter «var_global_domain_name» as the DNS domain name.
28. Enter «var_global_nameserver_ip» as the IP address for the first nameserver.
29. Answer n to finish entering DNS servers, or answer y to add up to two more DNS servers.
30. Answer n for running NIS client.
31. Press Enter to acknowledge the AutoSupport message.
32. Answer y to configuring the SP LAN interface.
33. Answer n to setting up DHCP on the SP LAN interface.
34. Enter «var_ntap_B_sp_int_ip» as the IP address for the SP LAN interface.
35. Enter «var_ntap_B_sp_int_netmask» as the subnet mask for the SP LAN interface.
36. Enter «var_ntap_B_sp_int_gw» as the IP address for the default gateway for the SP LAN interface.
37. Enter «var_ntap_mailhost_name» as the name for the mail host to receive SP messages and AutoSupport.
38. Enter «var_ntap_mailhost_ip» as the IP address for the mail host to receive SP messages and AutoSupport.

39. Enter «var_global_default_passwd» for the new administrative (root) password.
40. Enter «var_global_default_passwd» again to confirm the new administrative (root) password.
41. After these steps are completed, the controller should display a password prompt. Enter «var_global_default_passwd» to log in as root.

INSTALL DATA ONTAP TO ONBOARD FLASH STORAGE

Table 19) Install Data ONTAP to the onboard flash storage activity and verification.

Activity	Verification
Install Data ONTAP to the onboard flash storage. Duration: 10 minutes	Verify that the software was downloaded successfully by entering `software list` on the command line and verifying that the Data ONTAP zip file is present.

Controller A – «var_ntap_A_hostname»

1. Install the Data ONTAP image to the onboard flash device. `software install «var_ntap_data_ontap_url»`.
2. After this is complete, type download and press `Enter` to download the software to the flash device.

Controller B – «var_ntap_B_hostname»

1. Install the Data ONTAP image to the onboard flash device `software install «var_ntap_data_ontap_url»`.
2. After this is complete, type `download` and press `Enter` to download the software to the flash device.

HARDEN STORAGE SYSTEM LOGINS AND SECURITY

Table 20) Harden storage system logins and security activity and verification.

Activity	Verification
Harden storage system logins and security. Duration: 10 minutes	To verify that the root password has been set up, try to log in to the controller with the new credentials. To verify that telnet is disabled, try to access the controller by telnet; it should not connect. To verify that http access has been disabled, make sure that FilerView® must be accessed through https rather than through http.

Controller A – «var_ntap_A_hostname»

1. Type `secureadmin disable ssh`.
2. Type `secureadmin setup –f ssh` to enable ssh on the storage controller.
3. If prompted, type `yes` to rerun ssh setup.
4. Accept the default values for ssh1.x protocol.
5. Enter `1024` for ssh2 protocol.
6. Enter `yes` if the information specified is correct and to create the ssh keys.
7. Type `options telnet.enable off` to disable telnet on the storage controller.
8. Type `secureadmin setup ssl` to enable ssl on the storage controller.
9. If prompted, type `yes` to rerun ssl setup.

10. Enter the country name code, «var_global_ssl_country»; state or province name, «var_global_ssl_state»; locality name, «var_global_ssl_locality»; organization name, «var_global_ssl_org»; and organization unit name, «var_global_ssl_org_unit».
11. Enter «var_ntap_A_hostname».«var_global_domain_name» as the fully qualified domain name of the storage system.
12. Enter «var_ntap_admin_email_address» as the administrator's e-mail address.
13. Accept the default for days until the certificate expires.
14. Enter 1024 for the ssl key length.
15. Enter options httpd.admin.enable off to disable http access to the storage system.
16. Enter options httpd.admin.ssl.enable on to enable secure access to FilerView.

Controller B – «var_ntap_B_hostname»

1. Type secureadmin disable ssh.
2. Type secureadmin setup –f ssh to enable ssh on the storage controller.
3. If prompted, type yes to rerun ssh setup.
4. Accept the default values for ssh1.x protocol.
5. Enter 1024 for the ssh2.0 protocol.
6. Enter yes if the information specified is correct and to create the ssh keys.
7. Type options telnet.enable off to disable telnet on the storage controller.
8. Type secureadmin setup ssl to enable ssl on the storage controller.
9. If prompted, type yes to rerun ssl setup.
10. Enter the country name code, «var_global_ssl_country»; state or province name, «var_global_ssl_state»; locality name, «var_global_ssl_locality»; organization name, «var_global_ssl_org»; and organization unit name, «var_global_ssl_org_unit».
11. Enter «var_ntap_B_hostname».«var_global_domain_name» as the fully qualified domain name of the storage system.
12. Enter «var_ntap_admin_email_address» as the administrator's e-mail address.
13. Accept the default for days until the certificate expires.
14. Enter 1024 for the ssl key length.
15. Enter options httpd.admin.enable off to disable http access to the storage system.
16. Enter options httpd.admin.ssl.enable on to enable secure access to FilerView.

INSTALL REQUIRED LICENSES

Table 21) Install required licenses activity and verification.

Activity	Verification
Install required licenses. Duration: 5 minutes	To verify that the licenses installed correctly, enter the command license on the command line and verify that the licenses listed to the left are active.

Controller A – «var_ntap_A_hostname»

1. Install the necessary Data ONTAP licenses.

```
license add «var_ntap_cluster_lic» «var_ntap_fcp_lic»
«var_ntap_flash_cache_lic»
```

2. Type `license` to double-check the installed licenses.
3. Type reboot to reboot the storage controller.

Controller B – «var_ntap_B_hostname»

1. Install the necessary Data ONTAP licenses.

```
license add «var_ntap_cluster_lic» «var_ntap_fcp_lic»
«var_ntap_flash_cache_lic»
```

2. Type `license` to double-check the installed licenses.
3. Type reboot to reboot the storage controller.

ENABLE ACTIVE-ACTIVE CONTROLLER CONFIGURATION BETWEEN TWO STORAGE SYSTEMS

Table 22) Enable active-active controller configuration between the two storage systems activity and verification.

Activity	Verification
Enable active-active controller configuration between the two storage systems. Duration: 1 minute	Verify that clustering is enabled by entering the command `cf status` on both storage systems. Clustering should be enabled, and the partner and interconnect status should be set to `up`.

Controller A – «var_ntap_A_hostname» only

1. After both controllers have rebooted, type `cf enable` and press Enter to enable active-active controller configuration.

START FCP

Table 23) Start FCP activity and verification.

Activity	Verification
Start FCP.	No verification required.

On both controllers - «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Type `fcp start`.

SET UP STORAGE SYSTEM NTP TIME SYNCHRONIZATION

Table 24) Set up storage system NTP time synchronization activity and verification.

Activity	Verification
Set up storage system NTP time synchronization.	No verification required.

On both controllers - «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Type `date CCyymmddhhmm` where CCyy is the four-digit year, mm is the two-digit month, dd is the two-digit day of the month, hh is the two-digit hour, and the second mm is the two-digit minute to set the storage system time to the actual time.
2. Type `options timed.proto ntp` to synchronize with an NTP server.
3. Type `options timed.servers «var_global_ntp_server_ip»` to add the NTP server to the storage system list.

4. Type `options timed.enable on` to enable NTP synchronization on the storage system.

ADD IN-BAND MANAGEMENT INTERFACES TO 10GBE INTERFACES

Table 25) Add in-band management VLAN to 10GbE interfaces activity and verification.

Activity	Verification
Add in-band management interfaces to 10GbE interfaces. The IP addresses of these interfaces should be in the global FlexPod management VLAN. These interfaces must be added for the LACP interface group to become active and FCoE SAN Boot from storage to function correctly. Also, enable Cisco Discovery Protocol (CDP) on each storage controller. Duration: 10 minutes	Verify that the VLAN was added successfully by entering `ifconfig -a` on the command line and verifying that the VLAN interface is present. Also, enter `rdfile/etc/rc` on the command line and verify that the VLAN interface is present. CDP can be verified by typing `cdpd show-neighbors` a few minutes after enabling CDP.

Controller A – «var_ntap_A_hostname»

1. Type `vlan create vif0 «var_global_mgmt_vlan_id».`
2. Type `wrfile –a /etc/rc vlan create vif0 «var_global_mgmt_vlan_id».`
3. Type `ifconfig vif0-«var_global_mgmt_vlan_id» mtusize 1500 partner vif0-«var_global_mgmt_vlan_id».`
4. Type `wrfile –a /etc/rc ifconfig vif0-«var_global_mgmt_vlan_id» mtusize 1500 partner vif0-«var_global_mgmt_vlan_id».`
5. Type `ifconfig vif0-«var_global_mgmt_vlan_id» «var_ntap_A_ib_mgmt_IP» netmask «var_ntap_A_ib_mgmt_netmask».`
6. Type `wrfile –a ifconfig vif0-«var_global_mgmt_vlan_id» «var_ntap_A_ib_mgmt_IP» netmask «var_ntap_A_ib_mgmt_netmask».`
7. Type `options cdpd.enable on.`

Controller B – «var_ntap_B_hostname»

1. Type `vlan create vif0 «var_global_mgmt_vlan_id».`
2. Type `wrfile –a /etc/rc vlan create vif0 «var_global_mgmt_vlan_id».`
3. Type `ifconfig vif0-«var_global_mgmt_vlan_id» mtusize 1500 partner vif0-«var_global_mgmt_vlan_id».`
4. Type `wrfile –a /etc/rc ifconfig vif0-«var_global_mgmt_vlan_id» mtusize 1500 partner vif0-«var_global_mgmt_vlan_id».`
5. Type `ifconfig vif0-«var_global_mgmt_vlan_id» «var_ntap_B_ib_mgmt_IP» netmask «var_ntap_B_ib_mgmt_netmask».`
6. Type `wrfile –a ifconfig vif0-«var_global_mgmt_vlan_id» «var_ntap_B_ib_mgmt_IP» netmask «var_ntap_B_ib_mgmt_netmask».`
7. Type `options cdpd.enable on.`

CREATE DATA AGGREGATE AGGR1

Table 26) Create data aggregate `aggr1` activity and verification.

Activity	Verification
Create the data `aggregate aggr1.` Duration: 5 minutes	Verify that the aggregate was created successfully by entering the command `aggr status` on the command line and verify that the aggregate created is listed.

Controller A - «var_ntap_A_hostname»

1. Type `aggr create aggr1 –B 64 «var_ntap_A_num_disks_aggr1»` to create `aggr1` on the storage controller.

Note: In most cases, this command finishes quickly, but depending on the state of each disk, it might be necessary to zero some or all of the disks in order to add them to the aggregate. This might take up to 60 minutes to complete.

Controller B - «var_ntap_B_hostname»

1. Type `aggr create aggr1 –B 64 «var_ntap_B_num_disks_aggr1»` to create `aggr1` on the storage controller.

Note: In most cases, this command finishes quickly, but depending on the state of each disk, it might be necessary to zero some or all of the disks in order to add them to the aggregate. This might take up to 60 minutes to complete.

CREATE SNMP REQUESTS ROLE AND ASSIGN SNMP LOGIN PRIVILEGES

Table 27) Create SNMP requests role and assign SNMP login privileges activity and verification.

Activity	Verification
Create SNMP requests role and assign SNMP login privileges. Duration: 3 minutes	To verify, run the command `useradmin role list` on each of the storage controllers.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `useradmin role add «var_ntap_snmp_request_role» -a login-snmp`.

CREATE SNMP MANAGEMENT GROUP AND ASSIGN SNMP REQUEST ROLE

Table 28) Create SNMP management group and assign SNMP request role to its activity and verification.

Activity	Verification
Create SNMP management group and assign SNMP request role to it. Duration: 3 minutes	To verify, run the command `useradmin group list` on each of the storage controllers

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `useradmin group add «var_ntap_snmp_managers» -r «var_ntap_snmp_request_role»`.

CREATE SNMP USER AND ASSIGN IT TO SNMP MANAGEMENT GROUP

Table 29) Create SNMP user and assign it to SNMP management group activity and verification.

Activity	Verification
Create SNMP user and assign it to SNMP management group. Duration: 3 minutes	To verify, run the command `useradmin user list` on each of the storage controllers.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `useradmin user add «var_ntap_snmp_user» -g «var_ntap_snmp_managers»`.

Note: After the user is created, the system prompts for a password. Enter `«var_ntap_snmp_password»` when prompted.

ENABLE SNMP ON STORAGE CONTROLLERS

Table 30) Enable SNMP on the storage controller's activity and verification.

Activity	Verification
Enable SNMP on the storage controllers. Duration: 3 minutes	To verify, run the `command options snmp.enable` on each of the storage controllers.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `options snmp.enable on`.

SET UP SNMP V1 COMMUNITIES ON STORAGE CONTROLLERS

Table 31) Set up an SNMP v1 community on the storage controller's activity and verification.

Activity	Verification
Set up SNMP v1 communities on the storage controllers so that OnCommand System Manager can be used. Duration: 3 minutes	To verify, run the command `snmp community` on each of the storage controllers.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `snmp community delete all`.
2. Run the following command: `snmp community add ro «var_ntap_snmp_community».`

SET SNMP CONTACT INFORMATION FOR EACH STORAGE CONTROLLER

Table 32) Set SNMP contact information for each storage controller's activity and verification.

Activity	Verification
Set SNMP contact information for each of the storage controllers. Duration: 3 minutes	No verification required.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `snmp contact «var_ntap_admin_email_address»`.

SET SNMP LOCATION INFORMATION FOR EACH STORAGE CONTROLLER

Table 33) Set SNMP location information for each storage controller's activity and verification.

Activity	Verification
Set SNMP location information for each of the storage controllers. Duration: 3 minutes	No verification required.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `snmp location «var_ntap_snmp_site_name»`.

REINITIALIZE SNMP ON STORAGE CONTROLLERS

Table 34) Reinitialize SNMP on storage controller's activity and verification.

Activity	Verification
Reinitialize SNMP on the storage controllers. Duration: 3 minutes	No verification required.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Run the following command: `snmp init 1`.

ENABLE FLASH CACHE

Table 35) Enable Flash Cache activity and verification.

Activity	Verification
Enable Flash Cache. Duration: 1 minute	To verify that Flash Cache is turned on, issue the command `options flexscale.enable` and verify that its status is `on`.

Both controller A and B – «var_ntap_A_hostname» and «var_ntap_B_hostname»

1. Enter the following command to enable Flash Cache on each controller: `options flexscale.enable on`.

3.3 CISCO NEXUS 5548 DEPLOYMENT PROCEDURE: PART I

The following section provides a detailed procedure for configuring the Cisco Nexus 5548 switches for use in a FlexPod environment. Follow these steps precisely because failure to do so could result in an improper configuration.

Note: The Cisco Nexus 5548 switches should, at a minimum, be running NX-OS code release 5.0(3)N1(1c) in order for the 1Gb/sec SFPs to function properly.

Note: This configuration leverages the native VLAN on the trunk ports to discard untagged packets, by setting the native VLAN on the PortChannel, but not including this VLAN in the allowed VLANs on the PortChannel.

SET UP INITIAL CISCO NEXUS 5548 SWITCH (CONTROLLER A)

Table 36) Set up initial Cisco Nexus 5548 switch (controller A) activity and verification.

Activity	Verification
Initial Cisco Nexus 5548 switch setup. Duration: 60–75 minutes	No verification required.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. Upon initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.
2. Enter `yes` to enforce secure password standards.
3. Enter the password for the admin user.
4. Enter the password a second time to commit the password.
5. Enter `yes` to enter the basic configuration dialog.
6. Create another login account (yes/no) [`n`]: Enter.
7. Configure read-only SNMP community string (yes/no) [`n`]: Enter.
8. Configure read-write SNMP community string (yes/no) [`n`]: Enter.
9. Enter the switch name： «`var_nexus_A_hostname`» Enter.
10. Continue with out-of-band (mgmt0) management configuration? (yes/no) [`y`]: Enter.
11. Mgmt0 IPv4 address： «`var_nexus_A_mgmt0_IP`» Enter.
12. Mgmt0 IPv4 netmask： «`var_nexus_A_mgmt0_netmask`» Enter.
13. Configure the default gateway? (yes/no) [`y`]: Enter.
14. IPv4 address of the default gateway: «`var_nexus_A_mgmt0_gw`» Enter.
15. Enable the telnet service? (yes/no) [`n`]: Enter.
16. Enable the ssh service? (yes/no) [`y`]: Enter.
17. Type of ssh key you would like to generate (dsa/rsa):`rsa`.
18. Number of key bits <768–2048> `1024`: Enter.
19. Configure the ntp server? (yes/no) [`n`]: Enter.
20. Enter basic FC configurations (yes/no) [`n`]: Enter.
21. Would you like to edit the configuration? (yes/no) [`n`]: Enter.

Note: Be sure to review the configuration summary before enabling it.

22. Use this configuration and save it? (yes/no) [`y`]: Enter.

23. Configuration may be continued from the console or by using SSH. To use SSH, connect to «var_nexus_A_mgmt0_IP».
24. Log in as user admin with the password previously entered.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. Upon initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.
2. Enter yes to enforce secure password standards.
3. Enter the password for the admin user.
4. Enter the password a second time to commit the password.
5. Enter yes to enter the basic configuration dialog.
6. Create another login account (yes/no) [n]: Enter.
7. Configure read-only SNMP community string (yes/no) [n]: Enter.
8. Configure read-write SNMP community string (yes/no) [n]: Enter.
9. Enter the switch name: «var_nexus_B_hostname» Enter.
10. Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter.
11. Mgmt0 IPv4 address： «var_nexus_B_mgmt0_IP» Enter.
12. Mgmt0 IPv4 netmask: «var_nexus_B_mgmt0_netmask» Enter.
13. Configure the default gateway? (yes/no) [y]: Enter.
14. IPv4 address of the default gateway: «var_nexus_B_mgmt0_gw» Enter.
15. Enable the telnet service? (yes/no) [n]: Enter.
16. Enable the ssh service? (yes/no) [y]: Enter.
17. Type of ssh key you want to generate (dsa/rsa): rsa.
18. Number of key bits <768-2048>: 1024: Enter.
19. Configure the ntp server? (yes/no) [n]: Enter.
20. Enter basic FC configurations (yes/no) [n]: Enter.
21. Would you like to edit the configuration? (yes/no) [n]: Enter.

Note: Be sure to review the configuration summary before enabling it.

22. Use this configuration and save it? (yes/no) [y]: Enter.
23. Configuration may be continued from the console or by using SSH. To use SSH, connect to «var_nexus_B_mgmt0_IP».
24. Log in as user admin with the password previously entered.

ENABLE APPROPRIATE CISCO NEXUS LICENSING

Table 37) Enable the appropriate Cisco Nexus licensing activity and verification.

Activity	Verification
Enable the appropriate Cisco Nexus licensing. Duration: 3 minutes	Type show feature and verify that the appropriate licenses are enabled.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. Type config t to enter the global configuration mode.

2. Type `feature lacp`.
3. Type `feature fcoe`.
4. Type `feature npiv`.
5. Type `feature vpc`.
6. Type `feature fport-channel-trunk`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. Type `config t` to enter the global configuration mode.
2. Type `feature lacp`.
3. Type `feature fcoe`.
4. Type `feature npiv`.
5. Type `feature vpc`.
6. Type `feature fport-channel-trunk`.

SET GLOBAL CONFIGURATIONS

Table 38) Set global configurations activity and verification.

Activity	Verification
Set global configurations. Duration: 15 minutes	Use the `show run` command to view the global spanning-tree configuration.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `spanning-tree port type network default` to make sure that, by default, the ports are considered as network ports with regard to spanning tree.
2. Type `spanning-tree port type edge bpduguard default` to enable bpduguard on all edge ports by default.
3. Type `spanning-tree port type edge bpdufilter default` to enable bpdufilter on all edge ports by default.
4. Type `ntp server «var_global_ntp_server_ip» use-vrf management`.
5. Type `system jumbomtu 9000`.
6. Type `policy-map type network-qos jumbo`.
7. Type `class type network-qos class-default`.
8. Type `mtu 9000`.
9. Type `exit`.
10. Type `class type network-qos class-fcoe`.
11. Type `pause no-drop`.
12. Type `mtu 2158`.
13. Type `exit`.
14. Type `exit`.
15. Type `system qos`.
16. Type `service-policy type queuing input fcoe-default-in-policy`.
17. Type `service-policy type queuing output fcoe-default-out-policy`.

18. Type `service-policy type qos input fcoe-default-in-policy`.
19. Type `service-policy type network-qos jumbo`.
20. Type `exit`.
21. Type `copy run start`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `spanning-tree port type network default` to make sure that, by default, the ports are considered as network ports with regard to spanning-tree.
2. Type `spanning-tree port type edge bpduguard default` to enable bpduguard on all edge ports by default.
3. Type `spanning-tree port type edge bpdufilter default` to enable bpdufilter on all edge ports by default.
4. Type `ntp server «var_global_ntp_server_ip» use-vrf management`.
5. Type `system jumbomtu 9000`.
6. Type `policy-map type network-qos jumbo`.
7. Type `class type network-qos class-default`.
8. Type `mtu 9000`.
9. Type `exit`.
10. Type `class type network-qos class-fcoe`.
11. Type `pause no-drop`.
12. Type `mtu 2158`.
13. Type `exit`.
14. Type `exit`.
15. Type `system qos`.
16. Type `service-policy type queuing input fcoe-default-in-policy`.
17. Type `service-policy type queuing output fcoe-default-out-policy`.
18. Type `service-policy type qos input fcoe-default-in-policy`.
19. Type `service-policy type network-qos jumbo`.
20. Type `exit`.
21. Type `copy run start`.

CREATE NECESSARY VLANS

Table 39) Create necessary VLANs activity and verification.

Activity	Verification
Create necessary VLANs. Duration: 3 minutes	Use the `show vlan` command to show the list of VLANs that have been created on the switch.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. Type `vlan «var_global_mgmt_vlan_id»`.
2. Type `name MGMT-VLAN`.
3. Type `exit`.

4. Type `vlan «var_global_native_vlan_id»`.
5. Type `name Native-VLAN`.
6. Type `exit`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. Type `vlan «var_global_mgmt_vlan_id»`.
2. Type `name MGMT-VLAN`.
3. Type `exit`.
4. Type `vlan «var_global_native_vlan_id»`.
5. Type `name Native-VLAN`.
6. Type `exit`.

ADD INDIVIDUAL PORT DESCRIPTIONS FOR TROUBLESHOOTING

Table 40) Add individual port descriptions for troubleshooting activity and verification.

Activity	Verification
Add individual port descriptions for troubleshooting. Duration: 10 minutes	Use the `show interface status` command to print a list of ports and corresponding information, including configured port descriptions.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `interface Eth1/1`.
2. Type `description «var_ntap_A_hostname»:e2a`.
3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description «var_ntap_B_hostname»:e2a`.
6. Type `exit`.
7. Type `interface Eth1/5`.
8. Type `description «var_nexus_B_hostname»:Eth1/5`.
9. Type `exit`.
10. Type `interface Eth1/6`.
11. Type `description «var_nexus_B_hostname»:Eth1/6`.
12. Type `exit`.
13. Type `interface Eth1/3`.
14. Type `description «var_ucsm_A_hostname»:Eth1/19`.
15. Type `exit`.
16. Type `interface Eth1/4`.
17. Type `description «var_ucsm_B_hostname»:Eth1/19`.
18. Type `exit`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `interface Eth1/1`.
2. Type `description «var_ntap_A_hostname»:e2b`.

3. Type `exit`.
4. Type `interface Eth1/2`.
5. Type `description «var_ntap_B_hostname»:e2b`.
6. Type `exit`.
7. Type `interface Eth1/5`.
8. Type `description «var_nexus_A_hostname»:Eth1/5`.
9. Type `exit`.
10. Type `interface Eth1/6`.
11. Type `description «var_nexus_A_hostname»:Eth1/6`.
12. Type `exit`.
13. Type `interface Eth1/3`.
14. Type `description «var_ucsm_A_hostname»:Eth1/20`.
15. Type `exit`.
16. Type `interface Eth1/4`.
17. Type `description «var_ucsm_B_hostname»:Eth1/20`.
18. Type `exit`.

CREATE NECESSARY PORTCHANNELS

Table 41) Create necessary PortChannels activity and verification.

Activity	Verification
Create necessary PortChannels. Duration: 15 minutes	Use the `show interface status` command to verify that the appropriate PortChannel descriptions have been entered. Use the `show port-channel summary` command to verify that the correct individual ports have been added to the correct PortChannel.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.
4. Type `interface Eth1/5-6`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description «var_ntap_A_hostname»`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.

14. Type `exit`.
15. Type `interface Po12`.
16. Type `description «var_ntap_B_hostname»`.
17. Type `exit`.
18. Type `interface Eth1/2`.
19. Type `channel-group 12 mode active`.
20. Type `no shutdown`.
21. Type `exit`.
22. Type `interface Po13`.
23. Type `description «var_ucsm_A_hostname»`.
24. Type `exit`.
25. Type `interface Eth1/3`.
26. Type `channel-group 13 mode active`.
27. Type `no shutdown`.
28. Type `exit`.
29. Type `interface Po14`.
30. Type `description «var_ucsm_B_hostname»`.
31. Type `exit`.
32. Type `interface Eth1/4`.
33. Type `channel-group 14 mode active`.
34. Type `no shutdown`.
35. Type `exit`.
36. Type `copy run start`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `interface Po10`.
2. Type `description vPC peer-link`.
3. Type `exit`.
4. Type `interface Eth1/5-6`.
5. Type `channel-group 10 mode active`.
6. Type `no shutdown`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `description «var_ntap_A_hostname»`.
10. Type `exit`.
11. Type `interface Eth1/1`.
12. Type `channel-group 11 mode active`.
13. Type `no shutdown`.
14. Type `exit`.
15. Type `interface Po12`.

16. Type `description «var_ntap_B_hostname».`
17. Type `exit.`
18. Type `interface Eth1/2.`
19. Type `channel-group 12 mode active.`
20. Type `no shutdown.`
21. Type `exit.`
22. Type `interface Po13.`
23. Type `description «var_ucsm_A_hostname».`
24. Type `exit.`
25. Type `interface Eth1/3.`
26. Type `channel-group 13 mode active.`
27. Type `no shutdown.`
28. Type `exit.`
29. Type `interface Po14.`
30. Type `description «var_ucsm_B_hostname».`
31. Type `exit.`
32. Type `interface Eth1/4.`
33. Type `channel-group 14 mode active.`
34. Type `no shutdown.`
35. Type `exit.`
36. Type `copy run start.`

ADD PORTCHANNEL CONFIGURATIONS

Table 42) Add PortChannel configurations activity and verification.

Activity	Verification
Add PortChannel configurations. Duration: 15 minutes	Use the `show run interface <interface name>` command to show the configuration for a given interface or PortChannel.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `interface Po10.`
2. Type `switchport mode trunk.`
3. Type `switchport trunk native vlan «var_global_native_vlan_id».`
4. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
5. Type `spanning-tree port type network.`
6. Type `no shut.`
7. Type `exit.`
8. Type `interface Po11.`
9. Type `switchport mode trunk.`
10. Type `switchport trunk native vlan «var_global_native_vlan_id».`

11. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
12. Type `spanning-tree port type edge trunk.`
13. Type `no shut.`
14. Type `exit.`
15. Type `interface Po12.`
16. Type `switchport mode trunk.`
17. Type `switchport trunk native vlan «var_global_native_vlan_id».`
18. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
19. Type `spanning-tree port type edge trunk.`
20. Type `no shut.`
21. Type `exit.`
22. Type `interface Po13.`
23. Type `switchport mode trunk.`
24. Type `switchport trunk native vlan «var_global_native_vlan_id».`
25. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
26. Type `spanning-tree port type edge trunk.`
27. Type `no shut.`
28. Type `exit.`
29. Type `interface Po14.`
30. Type `switchport mode trunk.`
31. Type `switchport trunk native vlan «var_global_native_vlan_id».`
32. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
33. Type `spanning-tree port type edge trunk.`
34. Type `no shut.`
35. Type `exit.`
36. Type `copy run start.`

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `interface Po10.`
2. Type `switchport mode trunk.`
3. Type `switchport trunk native vlan «var_global_native_vlan_id».`
4. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
5. Type `spanning-tree port type network.`
6. Type `no shut.`
7. Type `exit.`
8. Type `interface Po11.`
9. Type `switchport mode trunk.`
10. Type `switchport trunk native vlan «var_global_native_vlan_id».`
11. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id».`
12. Type `spanning-tree port type edge trunk.`

13. Type `no shut`.
14. Type `exit`.
15. Type `interface Po12`.
16. Type `switchport mode trunk`.
17. Type `switchport trunk native vlan «var_global_native_vlan_id»`. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id»`.
18. Type `spanning-tree port type edge trunk`.
19. Type `no shut`.
20. Type `exit`.
21. Type `interface Po13`.
22. Type `switchport mode trunk`.
23. Type `switchport trunk native vlan «var_global_native_vlan_id»`.
24. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id»`.
25. Type `spanning-tree port type edge trunk`.
26. Type `no shut`.
27. Type `exit`.
28. Type `interface Po14`.
29. Type `switchport mode trunk`.
30. Type `switchport trunk native vlan «var_global_native_vlan_id»`.
31. Type `switchport trunk allowed vlan «var_global_mgmt_vlan_id»`.
32. Type `spanning-tree port type edge trunk`.
33. Type `no shut`.
34. Type `exit`.
35. Type `copy run start`.

CONFIGURE VIRTUAL PORTCHANNELS

Table 43) Configure vPCs activity and verification.

Activity	Verification
Configure vPCs. Duration: 10 minutes	Use the `show vpc` command on each switch to verify that each portchannel has been added to the appropriate vPC.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `vpc domain «var_nexus_vpc_domain_id»`.
2. Type `role priority 10`.
3. Type `peer-keepalive destination «var_nexus_B_mgmt0_IP» source «var_nexus_A_mgmt0_IP»`.
4. Type `exit`.
5. Type `interface Po10`.
6. Type `vpc peer-link`.
7. Type `exit`.

8. Type `interface Po11`.
9. Type `vpc 11`.
10. Type `exit`.
11. Type `interface Po12`.
12. Type `vpc 12`.
13. Type `exit`.
14. Type `interface Po13`.
15. Type `vpc 13`.
16. Type `exit`.
17. Type `interface Po14`.
18. Type `vpc 14`.
19. Type `exit`.
20. Type `copy run start`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `vpc domain «var_nexus_vpc_domain_id»`.
2. Type `role priority 20`.
3. Type `peer-keepalive destination «var_nexus_A_mgmt0_IP» source «var_nexus_B_mgmt0_IP»`.
4. Type `exit`.
5. Type `interface Po10`.
6. Type `vpc peer-link`.
7. Type `exit`.
8. Type `interface Po11`.
9. Type `vpc 11`.
10. Type `exit`.
11. Type `interface Po12`.
12. Type `vpc 12`.
13. Type `exit`.
14. Type `interface Po13`.
15. Type `vpc 13`.
16. Type `exit`.
17. Type `interface Po14`.
18. Type `vpc 14`.
19. Type `exit`.
20. Type `copy run start`.

LINK INTO EXISTING NETWORK INFRASTRUCTURE

Table 44) Uplink into existing network infrastructure activity and verification.

Activity	Verification
Uplink into existing network infrastructure. Duration: 15 minutes	No verification required.

Note: Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod environment. If an existing Cisco Nexus environment is present, NetApp recommends using vPCs to uplink the Cisco Nexus 5548 switches included in the FlexPod environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment.

SAVE CONFIGURATION

Table 45) Save configuration activity and verification.

Activity	Verification
Save the configuration.	No verification required.

On both Cisco Nexus 5548s – «var_nexus_A_hostname» and «var_nexus_B_hostname»

1. Type `copy run start`.

3.4 CISCO UNIFIED COMPUTING SYSTEM DEPLOYMENT PROCEDURE

The following section provides a detailed procedure for configuring the Cisco Unified Computing System for use in a FlexPod environment. These steps should be followed precisely because a failure to do so could result in an improper configuration.

PERFORM INITIAL SETUP OF THE CISCO UCS 6100 FABRIC INTERCONNECTS

Table 46) Initial setup of the Cisco UCS 6100 fabric interconnects activity and verification.

Activity	Verification
Initial setup of the Cisco UCS 6100 fabric interconnects. Duration: 5 minutes	Verify that the setup was successful by attempting to access the individual 6120s through the management IP addresses and the cluster IP address. The two 6120s should see each other as a clustered pair.

Cisco UCS 6120 A – «var_ucsm_A_hostname»

1. Connect to the console port on the first Cisco UCS 6100 fabric interconnect.
2. At the prompt to enter the configuration method, enter `console` to continue.
3. If asked to either do a new setup or restore from backup, enter `setup` to continue.
4. Enter `y` to continue to set up a new fabric interconnect.
5. Enter `y` to enforce strong passwords.
6. Enter «`var_global_default_passwd`» as the password for the admin user.
7. Enter the same password again to confirm the password for the admin user.
8. When asked if this fabric interconnect is part of a cluster, answer `y` to continue.

9. Enter `A` for the switch fabric.
10. Enter «`var_ucsm_cluster_hostname`» for the system name.
11. Enter «`var_ucsm_A_mgmt_ip`» for the Mgmt0 IPv4 address.
12. Enter «`var_ucsm_A_mgmt_netmask`» for the Mgmt0 IPv4 netmask.
13. Enter «`var_ucsm_A_mgmt_gw`» for the IPv4 address of the default gateway.
14. Enter «`var_ucsm_cluster_ip`» for the cluster IPv4 address.
15. To configure DNS, answer `y`.
16. Enter «`var_global_nameserver_ip`» for the DNS IPv4 address.
17. Answer `y` to set up the default domain name.
18. Enter «`var_global_domain_name`» for the default domain name.
19. Review the settings that were printed to the console, and if they are correct, answer `yes` to save the configuration.
20. Wait for the login prompt to make sure the configuration has been saved.

Cisco UCS 6120 B – «var_ucsm_B_hostname»

1. Connect to the console port on the second Cisco UCS 6100 fabric interconnect.
2. When prompted to enter the configuration method, enter `console` to continue.
3. The installer detects the presence of the partner fabric interconnect and adds this fabric interconnect to the cluster. Enter `y` to continue the installation.
4. Enter the admin password for the first fabric interconnect.
5. Enter «`var_ucsm_B_mgmt_ip`» for the Mgmt0 IPv4 address.
6. Answer yes to save the configuration.
7. Wait for the login prompt to confirm that the configuration has been saved.

LOG IN TO CISCO UCS MANAGER

Table 47) Log in to Cisco UCS Manager activity and verification.

Activity	Verification
Log in to Cisco UCS Manager. Duration: 3 minutes	Verify that the main window for the Cisco UCS Manager software shows up after clicking `Login`.

1. Open a Web browser and navigate to the Cisco UCS 6100 fabric extender's cluster address at «`var_ucsm_cluster_ip`».
2. Select the Launch link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter `admin` for the username and «`var_global_default_passwd`» as the password and click Login to log in to the Cisco UCS Manager software.

EDIT CHASSIS DISCOVERY POLICY

Table 48) Edit chassis discovery policy activity and verification.

Activity	Verification
Edit the chassis discovery policy.	No verification required.

1. Navigate to the `Equipment` tab in the left pane.
2. In the right pane, click the `Policies` tab.
3. Under `Global Policies`, change the `Chassis Discovery Policy` to `2-link`.
4. Click Save Changes in the bottom right corner.

ENABLE FIBRE CHANNEL, SERVER, AND UPLINK PORTS

Table 49) Enable Fibre Channel, server, and uplink ports activity and verification.

Activity	Verification
Enable Fibre Channel, server, and uplink ports. Duration: 5 minutes	Verify that the setup was successful by checking to see if all configured links show their status as `up`. This can also be verified on the Cisco Nexus side by running `show int status` and verifying that all ports connected to the Cisco UCS fabric interconnects are reported as `up`.

1. Select the Equipment tab on the top left of the window.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand the Unconfigured Ethernet Ports section.
4. Select ports 1 through 6 that are connected to the Cisco UCS chassis, right-click them, and select Configure as Server Port.
5. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
6. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select Configure as Uplink Port.
7. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
8. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Expansion Module 2.
9. Expand the Uplink FC Ports item and select FC ports 3 through 8.
10. Right-click and select Disable.
11. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
12. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
13. Expand the Unconfigured Ethernet Ports section.
14. Select ports 1 through 6 that are connected to the Cisco UCS chassis, right-click them, and select `Configure as Server Port`.
15. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
16. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select Configure as Uplink Port.
17. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
18. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Expansion Module 2.
19. Expand the Uplink FC Ports item and select FC ports 3 through 8.
20. Right click and select Disable to disable the ports.
21. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.

CREATE AN ORGANIZATION

Table 50) Create an organization activity and verification.

Activity	Verification
Create an organization. Duration: 2 minutes	Select Server tab > Service Profiles > root > Sub-Organizations on the left panel. The right panel displays the organization created.

1. From the New… menu at the top of the window, select Create Organization.
2. Enter «var_ucsm_infra_org_name» for the name of the organization.
3. Enter a description for the organization (optional).
4. Click OK.
5. In the message box that displays, click OK.

CREATE MAC ADDRESS POOLS

Table 51) Create MAC address pools activity and verification.

Activity	Verification
Create MAC address pools. Duration: 5 minutes	Select LAN tab > Pools > root. Select MAC Pools. It expands to show the MAC pools created. On the right panel, details of the MAC pools are displayed.

1. Select the LAN tab on the left of the window.
2. Under Pools, select root.

Note: Two MAC address pools are created, one for fabric A and one for fabric B.

3. Right-click MAC Pools under the root organization and select Create MAC Pool to create the MAC address pool for fabric A.
4. Enter MAC_Pool_A for the name of the MAC pool for fabric A.
5. (Optional) Enter a description of the MAC pool.
6. Click Next.
7. Click Add.
8. Specify a starting MAC address of «var_ucsm_mac_pool_A_start» for fabric A.

Note: The default is fine, but NetApp recommends changing the second-before-last octet to 0A to differentiate between MAC addresses in fabric A and fabric B (00:25:85:00:**0A**:00).

9. Specify a size of 32 for the MAC address pool for fabric A.
10. Click OK.
11. Click Finish.
12. In the message box that displays, click OK.
13. Right-click MAC Pools under the root organization and select Create MAC Pool to create the MAC address pool for fabric B.
14. Enter MAC_Pool_B for the name of the MAC pool for fabric B.
15. (Optional) Enter a description of the MAC pool.
16. Click Next.
17. Click Add.

18. Specify a starting MAC address of «var_ucsm_mac_pool_B_start» for fabric B.

Note: The default is fine, but NetApp recommends changing the second-before-last octet to 0B to differentiate between MAC addresses in fabric A and fabric B (00:25:85:00:**0B**:00).

19. Specify a size of 32 for the MAC address pool for fabric B.
20. Click OK.
21. Click Finish.
22. In the message box that displays, click OK.

CREATE VLANS

Table 52) Create VLANs activity and verification.

Activity	Verification
Create VLANs. Duration: 3 minutes	Select LAN tab > LAN Cloud > VLANs. Open VLANs and all of the created VLANs display underneath. The right panel shows the details for the individual VLANs.

1. Select the LAN tab on the left of the window.

Note: Two VLANs are created.

2. Right-click the VLANs item in the tree under LAN Cloud, and select Create VLAN(s).
3. Enter MGMT-VLAN as the name of the VLAN to be used for management traffic.
4. Keep the Common/Global option selected for the scope of the VLAN.
5. Enter a VLAN ID of «var_global_mgmt_vlan_id» for the management VLAN. Keep the sharing type as none.
6. Click OK, then OK.
7. Right-click the VLANs item in the tree and select Create VLAN(s).
8. Enter Native-VLAN as the name of the VLAN to be used for the native VLAN.
9. Keep the Common/Global option selected for the scope of the VLAN.
10. Enter a VLAN ID of «var_global_native_vlan_id» for the native VLAN.
11. Click OK, then OK.
12. In the VLAN list on the right, right-click the Native-VLAN and select Set as Native VLAN. Click Yes to confirm and click OK.

CREATE A NETWORK CONTROL POLICY

Table 53) Create a network control policy activity and verification.

Activity	Verification
Create a network control policy.	The newly created network control policy should be available.

1. Navigate to the LAN tab in the right pane.
2. Go to Policies > root.
3. Right-click Network Control Policy and click Create New Network Control Policy.
4. Use Enable_CDP as the name of the network control policy.

5. Change the `CDP` option to enabled. Leave Action on Uplink Fail set to link-down. Leave MAC Security Forge set to allow.
6. Click OK, then OK.

CREATE A VNIC TEMPLATE

Table 54) Create a vNIC template activity and verification.

Activity	Verification
Create vNIC template. Duration: 5 minutes	Select LAN tab > Policies > root >. Open the vNIC templates. The created vNICs display underneath. The right panel shows the details for the created vNIC templates.

1. Select the LAN tab on the left side of the window.
2. Go to Policies > root.

Note: Two vNIC templates are created, one for fabric A and one for fabric B.

3. Right-click vNIC Templates under the root organization and select Create vNIC Template.
4. Enter `vNIC_Template_A` as the name of the vNIC template for fabric A.
5. (Optional) Provide a description of the template.
6. Select Fabric A for the fabric ID.
7. Leave the target settings at the default values.
8. Select Updating Template under Template Type.
9. Under VLANs, check the MGMT-VLAN and Native-VLAN VLANs that were created previously.
10. Make sure that Native-VLAN is selected as the native VLAN.
11. Enter 9000 in the MTU box to enable jumbo frames.
12. Select MAC_Pool_A for fabric A under MAC Pool.
13. Select Enable_CDP from the drop-down menu under Network Control Policy.
14. Click OK, then OK to create the template.
15. Right-click vNIC Templates under the root organization and select Create vNIC Template.
16. Enter `vNIC_Template_B` as the name of the vNIC template for fabric B.
17. (Optional) Provide a description of the template.
18. Select Fabric B for the fabric ID.
19. Leave the target settings at the default values.
20. Select Updating Template under Template Type.
21. Under VLANs, check the MGMT-VLAN and Native-VLAN VLANs that were created previously.
22. Make sure that Native-VLAN is selected as the native VLAN.
23. Enter 9000 in the MTU box to enable jumbo frames.
24. Select the MAC_Pool_B for fabric B under MAC Pool.
25. Select Enable_CDP from the drop-down menu under Network Control Policy.
26. Click OK, then OK to create the template.

SET JUMBO FRAMES IN CISCO UCS FABRIC

Table 55) Set jumbo frames in Cisco UCS Fabric activity and verification.

Activity	Verification
Set jumbo frames in UCS fabric. Duration: 1 minute	Select LAN tab > LAN Cloud > QOS System Class.

1. Select the LAN tab on the left of the window.
2. Go to LAN Cloud > QoS System Class.
3. On the Best Effort Priority row, type 9000 in the MTU box and click the Save Changes button at the bottom of the screen.
4. Click OK to continue.

CREATE UPLINK PORTCHANNELS TO THE CISCO NEXUS 5548 SWITCHES

Table 56) Create uplink PortChannels to the Cisco Nexus 5548 switches activity and verification.

Activity	Verification
Create uplink PortChannels to the Cisco Nexus 5548 switches. Duration: 5 minutes	Log in, by using ssh, to each Cisco Nexus 5548 and issue `show vpc`. The status should show `Up` for each PortChannel.

1. Select the LAN tab on the left of the window.

Note: Two PortChannels are created, one from fabric A to both Cisco Nexus 5548 switches and one from fabric B to both Cisco Nexus 5548 switches.

2. Under LAN Cloud, expand the fabric A tree.
3. Right-click Port Channels and select Create Port Channel.
4. Enter `13` as the unique ID of the PortChannel.
5. Enter `Po13` as the name of the PortChannel.
6. Click Next.
7. Select ports 1/19 and 1/20 to be added to the PortChannel.
8. Click `>>` to add the ports to the PortChannel.
9. Click Finish to create the PortChannel.
10. In the message box, click OK to continue.
11. In the left pane, select the newly created PortChannel.
12. In the right pane under Actions, select Enable Port Channel.
13. In the pop-up box, click Yes, then OK to enable.
14. Expand the fabric B tree.
15. Right-click Port Channels and select Create Port Channel.
16. Enter `14` as the unique ID of the PortChannel.
17. Enter `Po14` as the name of the PortChannel.
18. Click `Next`.
19. Select ports 1/19 and 1/20 to be added to the PortChannel.

20. Click >> to add the ports to the PortChannel.
21. Click Finish to create the PortChannel.
22. In the message box, click OK to continue.
23. In the left pane, select the newly created PortChannel.
24. In the right pane under Actions, select Enable Port Channel.
25. In the pop-up box, click Yes, then OK to enable.

CREATE WWNN POOLS

Table 57) Create WWNN pools activity and verification.

Activity	Verification
Create WWNN pools. Duration: 5 minutes	The new name with the 256 block size displays in the right panel when WWNN pools is selected on the left panel.

1. Select the SAN tab at the top left of the window.
2. Select Pools > root.
3. Right-click WWNN Pools and select Create WWNN Pool.
4. Enter `WWNN_Pool` as the name of the WWNN pool.
5. (Optional) Add a description for the WWNN pool.
6. Click Next to continue.
7. The Add WWNN Blocks window displays; select Add at the bottom of the page.
8. The Create WWNN Block window displays; set the size of the WWNN block to `32`.
9. Click OK to proceed.
10. Click Finish to proceed.
11. Click OK to finish.

CREATE WWPN POOLS

Table 58) Create WWPN pools activity and verification.

Activity	Verification
Create WWPN pools. Duration: 5 minutes	The new name with the 256 block size displays in the right panel when WWPN pools is selected on the left panel. Also verify that the second-to-last octet reflects the fabric ID.

1. Select the SAN tab at the top left of the window.
2. Select Pools > root.

Note: Two WWPN pools are created, one for fabric A and one for fabric B.

3. Right-click WWPN Pools, and select Create WWPN Pool.
4. Enter `WWPN_Pool_A` as the name for the WWPN pool for fabric A.
5. (Optional) Give the WWPN pool a description.
6. Click Next.
7. Click Add to add a block of WWPNs.

8. Enter «var_ucsm_wwpn_pool_A_start» as the starting WWPN in the block for fabric A.

Note: The default is fine, but NetApp recommends changing the second-to-last octet to 0A to differentiate between WWPNs in fabric A and fabric B (20:00:00:25:B5:00:**0A**:00).

9. Set the size of the WWPN block to 32.
10. Click OK.
11. Click Finish to create the WWPN pool.
12. Click OK to proceed.
13. Right-click WWPN Pools and select Create WWPN Pool.
14. Enter WWPN_Pool_B as the name for the WWPN pool for fabric B.
15. (Optional) Give the WWPN pool a description.
16. Click Next.
17. Click Add to add a block of WWPNs.
18. Enter «var_ucsm_wwpn_pool_B_start» as the starting WWPN in the block for fabric B.

Note: The default is fine, but NetApp recommends changing the second-to-last octet to 0B to differentiate between WWPNs in fabric A and fabric B (20:00:00:25:B5:00:**0B**:01).

19. Set the size of the WWPN block to 32.
20. Click OK.
21. Click Finish to create the WWPN pool.
22. Click OK to proceed.

CREATE VSANS AND SAN PORTCHANNELS

Table 59) Create VSANs and SAN PortChannels activity and verification.

Activity	Verification
Create VSANs and SAN PortChannels. Duration: 5 minutes	Select SAN tab > SAN Cloud > VSANs on the left panel. The right panel displays the created VSANs.

1. Select the SAN tab at the top left of the window.
2. Expand the SAN cloud tree.
3. Right-click VSANs and select Create VSAN.
4. Enter VSAN_A as the VSAN name for fabric A.
5. Select Fabric A.
6. Enter «var_global_vsan_A_id» as the VSAN ID for fabric A.
7. Enter «var_global_fcoe_A_vlan_id» as the FCoE VLAN ID for fabric A.
8. Click OK and then OK to create the VSAN.
9. Right-click VSANs and select Create VSAN.
10. Enter VSAN_B as the VSAN name for fabric B.
11. Select Fabric B.
12. Enter «var_global_vsan_B_id» as the VSAN ID for fabric B.
13. Enter «var_global_fcoe_B_vlan_id» as the FCoE VLAN ID for fabric B.
14. Click OK and then OK to create the VSAN.
15. Select the SAN tab in the left window.

16. Select SAN Cloud > Fabric A> FC Port Channels.
17. Right-click and select Create Port Channel.
18. Click Yes and then enter `1` for the PortChannel ID and `SPo1` for the PortChannel name. Click Next.
19. Select ports 1 and 2 and click >> to add the ports to the PortChannel. Click Finish.
20. Click OK to complete creating the PortChannel.
21. Expand FC Port Channels and select the PortChannel just created. In the pull-down on the right side of the window select VSAN «`var_global_vsan_A_id`». Click Save Changes, then click OK.
22. Under Actions, click Enable Port Channel. Click Yes and then OK to enable the Port Channel. This action also enables the two FC ports in the PortChannel.
23. Select the SAN tab in the left window.
24. Select SAN Cloud > Fabric B> FC Port Channels.
25. Right-click and select Create Port Channel.
26. Click Yes, and then enter `2` for the PortChannel ID and `SPo2` for the PortChannel name. Click Next.
27. Select ports 1 and 2 and click >> to add the ports to the PortChannel. Click Finish.
28. Click OK to complete creating the PortChannel.
29. Expand FC Port Channels and select the PortChannel just created. In the pull-down on the right side of the window select VSAN «`var_global_vsan_B_id`». Click Save Changes, then click OK.
30. Under Actions, click Enable Port Channel. Click Yes, then OK to enable the PortChannel. This action also enables the two FC ports in the PortChannel.

CREATE VHBA TEMPLATES FOR FABRIC A AND B

Table 60) Create vHBA templates for fabric A and B activity and verification.

Activity	Verification
Create vHBA templates for fabric A and B. Duration: 3 minutes	Select SAN tab > Policies > root > vHBA Templates on the left panel. The right panel displays the created vHBAs. Each created vHBA is displayed under its respective template.

1. Select the SAN tab at the top left of the window.
2. Select Policies > root.

Note: Two vHBA templates are created, one for fabric A and one for fabric B.

3. Right-click vHBA Templates and select Create vHBA Template.
4. The Create vHBA Template window displays. Enter `vHBA_Template_A` as the name of the vHBA template for fabric A.
5. (Optional) Give the vHBA template a description.
6. Assign the vHBA template to fabric ID A.
7. Select VSAN_A as the VSAN for this vHBA template.
8. Select Initial Template for the Template Type.
9. Leave the Max Data Field Size at the default value (2048).
10. Select WWPN_Pool_A as the WWPN pool for this vHBA template.
11. Click OK to create the vHBA template.
12. Click OK in the pop-up box.
13. Right-click vHBA Templates and select Create vHBA Template.

14. The Create vHBA Template window displays. Enter `vHBA_Template_B` as the name of the vHBA template for fabric B.
15. (Optional) Give the vHBA template a description.
16. Assign the vHBA template to fabric ID B.
17. Select `VSAN_B` as the VSAN for this vHBA template.
18. Select Initial Template for the Template Type.
19. Leave the Max Data Field Size at the default value (2048).
20. Select WWPN_Pool_B as the WWPN pool for this vHBA template.
21. Click OK to create the vHBA template.
22. Click OK in the pop-up box.

CREATE BOOT POLICIES

Table 61) Create boot policies activity and verification.

Activity	Verification
Create boot policies (FCP must be initialized on the Cisco Nexus and FAS before starting this step). Duration: 15 minutes	Select Server tab > Policies > root > Boot Policies on the left panel and inspect the output on the right panel to make sure that all of the bootable devices are in the proper boot sequence order. The storage selection can be expanded to view the primary and secondary SAN targets. This procedure creates all four possible boot policies corresponding to the four possible primary boot ports on the two storage controllers.

1. Select the Servers tab at the top left of the window.
2. Select Policies > root.
3. Right-click Boot Policies and select Create Boot Policy.
4. Name the boot policy «`var_ntap_A_hostname`»`_2a`.
5. (Optional) Give the boot policy a description.
6. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
7. Expand the Local Devices drop-down menu and select Add CD-ROM.
8. Click the vHBA drop-down menu and select Add SAN Boot.
9. Enter `vHBA_A` in the vHBA field in the Add SAN Boot window that displays.
10. Make sure that Primary is selected as the type.
11. Click OK to add the SAN boot target.
12. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
13. Enter the WWPN for the primary FC adapter interface `2a` on the «`var_ntap_A_hostname`» controller. To obtain this information, log in to the «`var_ntap_A_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2a` and not the FC node name.

14. Keep the type as Primary.
15. Click OK to add the SAN boot target.
16. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.

17. Enter the WWPN for the primary FC adapter interface `2a` on the «`var_ntap_B_hostname`» controller. To obtain this information, log in to the «`var_ntap_B_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2a` and not the FC node name.

18. Click OK to add the SAN boot target.
19. Select Add SAN Boot under the vHBA drop-down menu.
20. Enter `vHBA_B` in the vHBA field in the Add SAN Boot window that displays.
21. The type should automatically be set to Secondary and it should be grayed out. This is fine.
22. Click OK to add the SAN boot target.
23. Select Add SAN Boot Target under the vHBA drop-down menu.
24. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.
25. Enter the WWPN for the primary FC adapter interface `2b` on the «`var_ntap_B_hostname`» controller. To obtain this information, log in to the «`var_ntap_B_hostname`» and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2b` and not the FC node name.

26. Keep the type as Primary.
27. Click OK to add the SAN boot target.
28. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
29. Enter the WWPN for the primary FC adapter interface `2b` on the «`var_ntap_A_hostname`» controller. To obtain this information, log in to the «`var_ntap_A_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2b` and not the FC node name.

30. Click OK to add the SAN boot target.
31. Click OK to create the boot policy in the Create Boot Policy pop-up window.
32. Select the Servers tab at the top left of the window.
33. Select Policies > root.
34. Right-click Boot Policies and select Create Boot Policy.
35. Name the boot policy «`var_ntap_B_hostname`»`_2b`.
36. (Optional) Give the boot policy a description.
37. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
38. Expand the Local Devices drop-down menu and select Add CD-ROM.
39. Click the vHBA drop-down menu and select Add SAN Boot.
40. Enter `vHBA_B` in the vHBA field in the Add SAN Boot window that displays.
41. Make sure that Primary is selected as the type.
42. Click OK to add the SAN boot target.
43. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
44. Enter the WWPN for the primary FC adapter interface `2b` on the «`var_ntap_B_hostname`» controller. To obtain this information, log in to the «`var_ntap_B_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2b` and not the FC node name.

45. Keep the type as Primary.
46. Click OK to add the SAN boot target.
47. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
48. Enter the WWPN for the primary FC adapter interface `2b` on the «`var_ntap_A_hostname`» controller. To obtain this information, log in to the «`var_ntap_A_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2b` and not the FC node name.

49. Click OK to add the SAN boot target.
50. Select Add SAN Boot under the vHBA drop-down menu.
51. Enter `vHBA_A` in the vHBA field in the Add SAN Boot window that displays.
52. The type should automatically be set to Secondary and it should be grayed out. This is fine.
53. Click OK to add the SAN boot target.
54. Select Add SAN Boot Target under the vHBA drop-down menu.
55. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.
56. Enter the WWPN for the primary FC adapter interface `2a` on the «`var_ntap_A_hostname`» controller. To obtain this information, log in to the «`var_ntap_A_hostname`» and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2a` and not the FC node name.

57. Keep the type as Primary.
58. Click OK to add the SAN boot target.
59. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LU`N` as 0.
60. Enter the WWPN for the primary FC adapter interface `2a` on the «`var_ntap_B_hostname`» controller. To obtain this information, log in to the «`var_ntap_B_hostname`» controller and run the `fcp show adapters` command.

Note: Be sure to use the FC portname for port `2a` and not the FC node name.

61. Click OK to add the SAN boot target.
62. Click OK to create the boot policy in the Create Boot Policy pop-up window.

CREATE SERVER POOLS

Table 62) Create server pools activity and verification.

Activity	Verification
Create server pools. Duration: 5 minutes	Select Servers tab >Pools > root > Sub-Organizations > «`var_ucsm_infra_org_name`» > Server Pool on the left panel. The right panel displays the servers assigned to the server pool. Because the service profile has not yet been created, no servers are assigned.

1. Select the Servers tab at the top left of the window.
2. Select Pools > root > Sub-Organizations > «`var_ucsm_infra_org_name`».
3. Right-click Server Pools and select Create Server Pool.
4. Name the server pool `Infra_Pool`.

5. (Optional) Give the server pool a description.
6. Click Next to continue to add servers.
7. Select two B200 servers to be added to the Infra_Pool server pool. Click >> to add them to the pool.
8. Click Finish to create the server pool.
9. The Create Server Pool window displays. Select OK to proceed.

CREATE UUID SUFFIX POOLS

Table 63) Create UUID suffix pools activity and verification.

Activity	Verification
Create UUID suffix pools. Duration: 3 minutes	Select Servers tab > Select Pools > root > Sub-Organizations > «var_ucsm_infra_org_name» > Server Pools > UUID Suffix Pools on the left panel. The right panel displays the UUID suffix pools available. Make sure that the UUID suffix pools created are displayed.

1. Select the Servers tab on the top left of the window.
2. Select Pools > root.
3. Right-click UUID Suffix Pools and select Create UUID Suffix Pool.
4. Name the UUID suffix pool UUID_Pool.
5. (Optional) Give the UUID suffix pool a description.
6. Leave the prefix at the derived option.
7. Click Next to continue.
8. The Create UUID Suffix Pool Add UUID Blocks window displays. Click the Add button at the bottom of the window to add a block of UUID suffixes.
9. The From field is fine at the default setting.
10. Set the size of the UUID suffix pool to 32. Click OK.
11. Click Finish to create the UUID suffix pool.
12. Click OK in the pop-up box to proceed.

CREATE SERVICE PROFILE TEMPLATES

Note: This section details the creation of two service profile templates: one for fabric A and one for fabric B.

Table 64) Create service profile templates activity and verification.

Activity	Verification
Create service profile templates.	Select Servers tab then Service Profile Templates > root > Sub-Organizations > «var_ucsm_infra_org_name» > Service Template. Expand the individual items to reveal the created objects. Make sure that all of the vHBAs and vNICs were created.

1. Select the Servers tab at the top left of the window.
2. Select Service Profile Templates > root > Sub-Organizations > «var_ucsm_infra_org_name».
3. In the right window, click the Create Service Profile Template under the Actions section.

4. The Create Service Profile Template window displays.
   a. Identify the Service Profile Template Section.
      i. Name the service profile template «var_ntap_A_hostname»_2a. This service profile template is configured to boot from controller A – «var_ntap_A_hostname».
      ii. Keep the type at Initial Template.
      iii. In the UUID section, select UUID_Pool as the UUID pool.
      iv. Click Next to continue to the next section.
   b. Storage section
      i. Select default for the Local Storage field.
      ii. Select the Expert option for the How would you like to configure SAN connectivity field.
      iii. In the WWNN Assignment field, select WWNN_Pool.
      iv. Click the Add button at the bottom of the window to add vHBAs to the template.
      v. The Create vHBA window displays. Name the vHBA vHBA_A.
      vi. Check the box for Use SAN Connectivity Template.
      vii. Select vHBA_Template_A in the vHBA Template field.
      viii. Select the appropriate operating system in the Adapter Policy field.
      ix. Click OK to add the vHBA to the template.
      x. Click the Add button at the bottom of the window to add vHBAs to the template.
      xi. The Create vHBA window displays. Name the vHBA vHBA_B.
      xii. Check the box for Use SAN Connectivity Template.
      xiii. Select vHBA_Template_B in the vHBA Template field.
      xiv. Select the appropriate operating system in the Adapter Policy field.
      xv. Click OK to add the vHBA to the template.
      xvi. Verify – Review the table to make sure that both of the vHBAs were created.
      xvii. Click Next to continue to the next section.
   c. Networking Section
      i. Leave the Dynamic vNIC Connection Policy field at the default.
      ii. Select Expert for the How would you like to configure LAN connectivity? option.
      iii. Click Add to add a vNIC to the template.
      iv. The Create vNIC window displays. Name the vNIC vNIC_A.
      v. Check the Use LAN Connectivity Template checkbox.
      vi. Select vNIC_Template_A for the vNIC Template field.
      vii. Select the appropriate operating system for the Adapter Policy field.
      viii. Click OK to add the vNIC to the template.
      ix. Click Add to add a vNIC to the template.
      x. The Create vNIC window displays. Name the vNIC vNIC_B.
      xi. Check the Use LAN Connectivity Template checkbox.
      xii. Select vNIC_Template_B for the vNIC Template field.
      xiii. Select the appropriate operating system for the Adapter Policy field.
      xiv. Click OK to add the vNIC to the template.
      xv. Verify: Review the table to make sure that both of the vNICs were created.
      xvi. Click Next to continue to the next section.
   d. vNIC/vHBA Placement Section
      i. Keep the default of Let System Perform Placement in the Select Placement field.
      ii. Verify: Review the table to make sure that all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not important.
      iii. Click Next to continue to the next section.
   e. Server Boot Order Section
      i. Select «var_ntap_A_hostname»_2a in the Boot Policy field.
      ii. Verify: Review the table to make sure that all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
      iii. Click Next to continue to the next section.

f. Maintenance Policy Section
   i. Keep the default of no policy used by default.
   ii. Click Next to continue to the next section.

g. Server Assignment Section
   i. Select `Infra_Pool` in the Server Assignment field.
   ii. Keep the default of `<not set>` for the Server Pool Qualification field.
   iii. Select `Down` for the power state.
   iv. Click `Next` to continue to the next section.

h. Operational Policies Section
   i. Configuration is not needed here (accept defaults).
   ii. Click Finish to create the Service Profile template.
   iii. Click OK in the pop-up window to proceed.

5. In the right window, click the Create Service Profile Template under the Actions section. The Create Service Profile Template window displays.

   a. Identify Service Profiles Template section.
      i. Name the service profile template «`var_ntap_B_hostname`»`_2b`. This service profile template is configured to boot from controller B – «`var_ntap_B_hostname`».
      ii. Keep the type at Initial Template.
      iii. In the UUID section, select `UUID_Pool` as the UUID pool.
      iv. Click Next to continue to the next section.

   b. Storage section
      i. Select default for the Local Storage field.
      ii. Select the Expert option for the How would you like to configure SAN connectivity? field.
      iii. In the WWNN Assignment field, select `WWNN_Pool`.
      iv. Click the Add button at the bottom of the window to add vHBAs to the template.
      v. The Create vHBA window displays. Name the vHBA `vHBA_A`.
      vi. Check the box for Use SAN Connectivity Template.
      vii. Select `vHBA_Template_A` in the vHBA Template field.
      viii. Select the appropriate operating system in the Adapter Policy field.
      ix. Click OK to add the vHBA to the template.
      x. Click the Add button at the bottom of the window to add vHBAs to the template.
      xi. The Create vHBA window displays. Name the vHBA `vHBA_B`.
      xii. Check the box for Use SAN Connectivity Template.
      xiii. Select `vHBA_Template_B` in the vHBA Template field.
      xiv. Select the appropriate operating system in the Adapter Policy field.
      xv. Click OK to add the vHBA to the template.
      xvi. Verify: Review the table to make sure that both of the vHBAs were created.
      xvii. Click Next to continue to the next section.

   c. Networking Section
      i. Leave the Dynamic vNIC Connection Policy field at the default.
      ii. Select Expert for the How would you like to configure LAN connectivity? option.
      iii. Click Add to add a vNIC to the template.
      iv. The Create vNIC window displays. Name the vNIC `vNIC_A`.
      v. Check the Use LAN Connectivity Template checkbox.
      vi. Select `vNIC_Template_A` for the vNIC Template field.
      vii. Select the appropriate OS for the Adapter Policy field.
      viii. Click OK to add the vNIC to the template.
      ix. Click Add to add a vNIC to the template.
      x. The Create vNIC window displays. Name the vNIC `vNIC_B`.
      xi. Check the Use LAN Connectivity Template checkbox.
      xii. Select `vNIC_Template_B` for the vNIC Template field.

xiii. Select the appropriate operating system for the Adapter Policy field.
xiv. Click OK to add the vNIC to the template.
xv. Verify: Review the table to make sure that both of the vNICs were created.
xvi. Click Next to continue to the next section.

d. vNIC/vHBA Placement Section
   i. Keep the default of Let System Perform Placement in the Select Placement field.
   ii. Verify: Review the table to make sure that all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not important.
   iii. Click Next to continue to the next section.

e. Server Boot Order Section
   i. Select «var_ntap_B_hostname»_2b in the Boot Policy field.
   ii. Verify: Review the table to make sure that all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
   iii. Click Next to continue to the next section.

f. Maintenance Policy Section
   i. Keep the default of no policy used by default.
   ii. Click Next to continue to the next section.

g. Server Assignment Section
   i. Select Infra_Pool in the Server Assignment field.
   ii. Keep the default of <not set> for the Server Pool Qualification field.
   iii. Select Down for the power state.
   iv. Click Next to continue to the next section.

h. Operational Policies Section
   i. Configuration is not needed here (accept defaults).

i. Click Finish to create the Service Profile template.

j. Click OK in the pop-up window to proceed.

CREATE SERVICE PROFILES

Table 65) Create service profiles activity and verification.

Activity	Verification
Create service profiles.	Select Server tab > Service Profile > root > Sub-Organizations > «var_ucsm_infra_org_name» and make sure that two total service profiles were created; two for each storage system.

1. Select the Servers tab at the top left of the window.
2. Select Service Profile Templates > root > Sub-Organizations > «var_ucsm_infra_org_name».
3. Click Create Service Profiles From Template in the Actions section of the right main window.
4. Enter ucs_host_«var_ntap_A_hostname»_2a for the service profile prefix.
5. Enter 1 for the number of service profiles to create.
6. Select «var_ntap_A_hostname»_2a for the Service Profile Template field. It should be under Organizations > root > Sub-Organizations > «var_ucsm_infra_org_name».
7. Click OK to create the service profile.
8. Click OK in the message box.
9. Select the Servers tab at the top left of the window.
10. Select Service Profile Templates > root > Sub-Organizations >«var_ucsm_infra_org_name».

11. Click Create Service Profiles From Template in the Actions section of the right main window.
12. Enter `ucs_host_«var_ntap_B_hostname»_2b` for the service profile prefix.
13. Enter 1 for the number of Service Profiles to create.
14. Select `«var_ntap_B_hostname»_2b` for the Service Profile Template field. It should be under Organizations > root > Sub-Organizations > `«var_ucsm_infra_org_name»`.
15. Click OK to create the service profile.
16. Click OK in the message box.

ADD A BLOCK OF IP ADDRESSES FOR KVM ACCESS

Table 66) Add a block of IP addresses for KVM access activity and verification.

Activity	Verification
Add a block of IP addresses for KVM access.	No verification required.

1. Navigate to the Admin tab in the left pane and then to Communication Management.
2. Right-click Management IP Pool and select Create Block of IP Addresses.
3. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
4. Click OK to create the IP block.

SYNCHRONIZE CISCO UCS TO NTP

Table 67) Synchronize Cisco UCS to NTP activity and verification.

Activity	Verification
Synchronize Cisco UCS to NTP.	No verification required.

1. Navigate to the Admin tab in the left pane and then to Timezone Management.
2. Select the appropriate timezone in the Timezone drop-down menu.
3. Click Save Changes and then OK.
4. Click Add NTP Server.
5. Input `«var_global_ntp_server_ip»` and click OK.

ADD MORE BLADES TO FLEXPOD UNIT

Table 68) Add more blades to FlexPod unit activity and verification.

Activity	Verification
Add more blades to the FlexPod unit.	No verification required.

Add server pools, service profile templates, and service profiles in the respective organizations to add more servers to the FlexPod unit. All other pools and policies are at the root level and can be shared among the organizations.

3.5 GATHER NECESSARY INFORMATION

After the Cisco UCS service profiles have been created (in the previous steps), the infrastructure blades in the environment each have a unique configuration. To proceed with the FlexPod deployment, specific

information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information in Table 69 and Table 70.

Table 69) NetApp FAS3240A FC portname information.

NetApp Controller	FC Port	FC Portname
NetApp FAS3240A – «var_ntap_A_hostname»	2a	
	2b	
NetApp FAS3240B – «var_ntap_B_hostname»	2a	
	2b	

Note: On each NetApp controller, use `show fcp adapters` to gather the information in Table 69.

Table 70) Cisco UCS blade WWPN information.

Cisco UCS Service Profile Name	vHBA_A WWPN	vHBA_B WWPN
ucs_host_«var_ntap_A_hostname»_2a1		
ucs_host_«var_ntap_B_hostname»_2a1		

Note: To gather the information in Table 70, launch the Cisco UCS Manager GUI, and in the left pane select the `Servers` tab. From there, expand Servers > Service Profiles > root > Sub_Organizations > «var_ucsm_infra_org_name». Click each service profile and then click the `Storage` tab on the right. While doing so, record the WWPN information in the right display window for both vHBA_A and vHBA_B for each service profile in Table 70.

3.6 CISCO NEXUS 5548 DEPLOYMENT PROCEDURE: PART II

Table 71 contains the procedural steps for the second part of the Cisco Nexus 5548 deployment.

CREATE VSANS, ASSIGN FC PORTS, TURN ON FC PORTS

Table 71) Create VSANs, assign FC ports to SAN PortChannels and appropriate VSANs, and turn on FC ports activity and verification.

Activity	Verification
Create VSANs, assign FC ports to SAN PortChannels and appropriate VSANs, and turn on FC ports. Duration: 5 minutes	Verify the successful creation of the VSANs and the assignment of the FC ports by issuing the command `show run`, and verify that the VSANs and the mapped ports are shown.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `vlan «var_global_fcoe_A_vlan_id»`.
2. Type `name FCoE_Fabric_A`.
3. Type `fcoe vsan «var_global_vsan_A_id»`.
4. Type `exit`.
5. Type `interface po11`.
6. Type `switchport trunk allowed vlan add «var_global_fcoe_A_vlan_id»`.
7. Type `exit`.
8. Type `interface vfc11`.
9. Type `bind interface po11`.
10. Type `no shutdown`.
11. Type `exit`.
12. Type `interface po12`.
13. Type `switchport trunk allowed vlan add «var_global_fcoe_A_vlan_id»`.
14. Type `exit`.
15. Type `interface vfc12`.
16. Type `bind interface po12`.
17. Type `no shutdown`.
18. Type `exit`.
19. Type `interface san-port-channel 1`.
20. Type `channel mode active`.
21. Type `exit`.
22. Type `vsan database`.
23. Type `vsan «var_global_vsan_A_id» name Fabric_A`.
24. Type `vsan «var_global_vsan_A_id» interface fc2/1-2`.
25. Type `vsan «var_global_vsan_A_id» interface san-port-channel 1`.
26. Type `vsan «var_global_vsan_A_id» interface vfc11`.
27. Type `vsan «var_global_vsan_A_id» interface vfc12`.
28. Type `exit`.
29. Type `interface fc2/1-2`.
30. Type `channel-group 1 force`.

31. Type `no shutdown`.
32. Type `exit`.

Cisco Nexus 5548 B - «var_nexus_B_hostname»

1. From the global configuration mode, type `vlan «var_global_fcoe_B_vlan_id»`.
2. Type `name FCoE_Fabric_B`.
3. Type `fcoe vsan «var_global_vsan_B_id»`.
4. Type `exit`.
5. Type `interface po11`.
6. Type `switchport trunk allowed vlan add «var_global_fcoe_B_vlan_id»`.
7. Type `exit`.
8. Type `interface vfc11`.
9. Type `bind interface po11`.
10. Type `no shutdown`.
11. Type `exit`.
12. Type `interface po12`.
13. Type `switchport trunk allowed vlan add «var_global_fcoe_B_vlan_id»`.
14. Type `exit`.
15. Type `interface vfc12`.
16. Type `bind interface po12`.
17. Type `no shutdown`.
18. Type `exit`.
19. Type `interface san-port-channel 2`.
20. Type `channel mode active`.
21. Type `exit`.
22. Type `vsan database`.
23. Type `vsan «var_global_vsan_B_id» name Fabric_B`.
24. Type `vsan «var_global_vsan_B_id» interface fc2/1-2`.
25. Type `vsan «var_global_vsan_B_id» interface san-port-channel 2`.
26. Type "`vsan «var_global_vsan_B_id» interface vfc11`.
27. Type `vsan «var_global_vsan_B_id» interface vfc12`.
28. Type `exit`.
29. Type `interface fc2/1-2`.
30. Type `channel-group 2 force`.
31. Type `no shutdown`.
32. Type `exit`.

CREATE DEVICE ALIASES AND CREATE ZONES

Table 72) Create device aliases on each Cisco Nexus 5548 and create zones for each Cisco UCS host activity and verification.

Activity	Verification
Create device aliases on each Cisco Nexus 5548 and create zones for each Cisco UCS host. Duration: 30 minutes	Verify that the entries were successfully entered into the device alias database by entering `show device-alias`. Verify that the zones are correct by issuing the command `show zoneset`. The output should show the zoneset and the zones that were added to the zoneset.

Cisco Nexus 5548 A – «var_nexus_A_hostname»

1. From the global configuration mode, type `device-alias database`.
2. Type `device-alias name ucs_host_«var_ntap_A_hostname»_2a1_A pwwn <vHBA_A WWPN>`.
3. Type `device-alias name ucs_host_«var_ntap_B_hostname»_2b1_A pwwn <vHBA_A WWPN>`.
4. Type `device-alias name «var_ntap_A_hostname»_2a pwwn <2a WWPN>`.
5. Type `device-alias name «var_ntap_B_hostname»_2a pwwn <2a WWPN>`.

Note: Get this information from Table 69 and Table 70.

6. After all of the necessary device-alias are created, type `exit`.
7. Type `device-alias commit`.
8. Create the zones for each service profile.
   a. Type `zone name ucs_host_«var_ntap_A_hostname»_2a1_A vsan «var_global_vsan_A_id»`.
   b. Type `member device-alias ucs_host_«var_ntap_A_hostname»_2a1_A`.
   c. Type `member device-alias «var_ntap_A_hostname»_2a`.
   d. Type `member device-alias «var_ntap_B_hostname»_2a`.
   e. Type `exit`.
   f. Type `zone name ucs_host_«var_ntap_B_hostname»_2b1_A vsan «var_global_vsan_A_id»`.
   g. Type `member device-alias ucs_host_«var_ntap_B_hostname»_2b1_A`.
   h. Type `member device-alias «var_ntap_B_hostname»_2a`.
   i. Type `member device-alias «var_ntap_A_hostname»_2a`.
   j. Type `exit`.
9. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
10. Create the zoneset and add the necessary members.
    a. Type `zoneset name flexpod vsan «var_global_vsan_A_id»`.
    b. Type `member ucs_host_«var_ntap_A_hostname»_2a1_A`.
    c. Type `member ucs_host_«var_ntap_B_hostname»_2b1_A`.
    d. Type `exit`.

11. Activate the zoneset.
    a. Type `zoneset activate name flexpod vsan «var_global_vsan_A_id»`.
    b. Type `exit`.
12. Type `copy run start`.

Cisco Nexus 5548 B – «var_nexus_B_hostname»

1. From the global configuration mode, type `device-alias database`.
2. Type `device-alias name ucs_host_«var_ntap_A_hostname»_2a1_B pwwn <vHBA_B WWPN>`.
3. Type `device-alias name ucs_host_«var_ntap_B_hostname»_2b1_B pwwn <vHBA_B WWPN>`.
4. Type `device-alias name «var_ntap_A_hostname»_2b pwwn <2b WWPN>`.
5. Type `device-alias name «var_ntap_B_hostname»_2b pwwn <2b WWPN>`.

Note: Get this information from the tables in the previous section.

6. After all of the necessary device-alias are created, type `exit`.
7. Type `device-alias commit`.
8. Create the zones for each service profile.
    a. Type `zone name ucs_host_«var_ntap_A_hostname»_2a1_B vsan «var_global_vsan_B_id»`.
    b. Type `member device-alias ucs_host_«var_ntap_A_hostname»_2a1_B`.
    c. Type `member device-alias «var_ntap_B_hostname»_2b`.
    d. Type `member device-alias «var_ntap_A_hostname»_2b`.
    e. Type `exit`.
    f. Type `zone name ucs_host_«var_ntap_B_hostname»_2b1_B vsan «var_global_vsan_B_id»`.
    g. Type `member device-alias ucs_host_«var_ntap_B_hostname»_2b1_B`.
    h. Type `member device-alias «var_ntap_A_hostname»_2b`.
    i. Type `member device-alias «var_ntap_B_hostname»_2b`.
    j. Type `exit`.
9. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
10. Create the zoneset and add the necessary members.
    a. Type `zoneset name flexpod vsan «var_global_vsan_B_id»`.
    b. Type `member ucs_host_«var_ntap_A_hostname»_2a1_B`.
    c. Type `member ucs_host_«var_ntap_B_hostname»_2b1_B`.
    d. Type `exit`.
11. Activate the zoneset.
    a. Type `zoneset activate name flexpod vsan «var_global_vsan_B_id»`.
    b. Type `exit`.
12. Type `copy run start`.

4 REFERENCES

- NetApp Support (formerly NOW®) site
- NetApp FAS3200 Family
- Cisco Nexus 5548 Switch
- Cisco Unified Computing System

5 REVISION HISTORY

Version	Revision Comments
1.0	January 2012 Original document

6 AUTHORS

John George, Reference Architect, Infrastructure and Cloud Engineering, NetApp

John George is a reference architect in the NetApp Infrastructure and Cloud Engineering team and is focused on developing, validating, and supporting cloud infrastructure solutions that include NetApp products. Before his current role, he supported and administered Nortel's worldwide training network and VPN infrastructure. John holds a master's degree in computer engineering from Clemson University.

Chris Reno, Reference Architect, Infrastructure and Cloud Engineering, NetApp

Chris Reno is a reference architect in the NetApp Infrastructure and Cloud Enablement team and is focused on creating, validating, supporting, and evangelizing solutions based on NetApp products. Before his current role, he worked with NetApp product engineers designing and developing innovative ways to do Q&A for NetApp products, including enablement of a large grid infrastructure using physical and virtualized compute resources. In these roles, Chris gained expertise in stateless computing, netboot architectures, and virtualization. Chris has his bachelor of science degree in international business and finance and his bachelor of arts degree in Spanish from the University of North Carolina – Wilmington while also holding numerous industry certifications.

Lindsey Street, Systems Architect, Infrastructure and Cloud Engineering, NetApp

Lindsey Street is a systems architect in the NetApp Infrastructure and Cloud Engineering team. She focuses on the architecture, implementation, compatibility, and security of innovative vendor technologies to develop competitive and high-performance end-to-end cloud solutions for customers. Lindsey started her career in 2006 at Nortel as an interoperability test engineer, testing customer equipment interoperability for certification. Lindsey has her bachelor of science degree in computer networking and her master of science in information security from East Carolina University.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

© Copyright 2012 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, AutoSupport, Data ONTAP, FilerView, FlexPod, NOW, and OnCommand are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Cisco and Cisco Nexus are registered trademarks and Cisco UCS and Cisco Unified Computing System are trademarks of Cisco Systems, Inc. VMware is a registered trademark and View is a trademark of VMware, Inc. Microsoft is a registered trademark of Microsoft Corporation. Mac is a registered trademark of Apple, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.TR-4019-0112

www.netapp.com